CHAPTER 32

ENTERPRISE RISK MANAGEMENT, CRISIS PREPAREDNESS, AND ORGANIZATIONAL RESILIENCE

Sixbert SANGWA
African Leadership University | Kigali, Rwanda | ssangwa@alueducation.com

PARENT BOOK AND IDENTIFIER
The Business Enterprise: Core Functions, Integrated Management, and Emerging Transformations
https://doi.org/10.65655/ocp.m30

VOLUME EDITOR AND PUBLISHER
Prof. Dr. Placide MUTABAZI
Open Christian Press, imprint of Open Christian University and Center for Faith and Work

CHAPTER IDENTIFIER
10.65655/ocp.m30.c141

COPYRIGHTS AND LICENSE
© 2026 Sixbert SANGWA | CC BY 4.0

ABSTRACT

Enterprise risk management (ERM) is frequently organized around risk inventories, yet an inventory cannot explain how several individually manageable disruptions combine to threaten the continued delivery of essential services. This chapter conceptualizes risk management as the governance of uncertainty across strategically interconnected enterprise functions and organizational resilience as a context-dependent capability to anticipate, withstand, respond to, recover from, and learn through disturbances. Drawing on a purposive, critical synthesis of foundational scholarship, peer-reviewed research, professional guidance, and official Rwandan evidence available by 3 November 2026, it examines twelve approved domains spanning risk governance, strategic and financial exposures, operations, technology, people, assessment methods, business continuity, interconnected crises, and adaptive recovery. The analysis contrasts decision-theoretic, enterprise-wide, high-reliability, resilience, contingency, and real-options perspectives, explicitly identifying the assumptions that limit their application. Rwanda's enterprise statistics and documented flood disruptions provide institutional grounding without being misrepresented as firm-level causal evidence. A constructed Kigali distributor case integrates an auditable risk register, business impact analysis, continuity arrangements, cash stress test, expected-loss comparison, and exercise schedule. Comparative discussion of international standards distinguishes voluntary guidance from binding obligations and examines the costs of transferring complex systems to resource-constrained firms. The chapter argues that defensible resilience is neither the elimination of uncertainty nor the duplication of every resource; it is a continually tested alignment of decision rights, essential services, financial capacity, information, relationships, and ethically legitimate recovery priorities. Its integrative propositions are conceptual rather than empirically validated.

Keywords: enterprise risk management; risk governance; organizational resilience; business impact analysis; business continuity; crisis management; systemic risk; stress testing; supply-chain disruption; Rwanda.

LEARNING OUTCOMES AND CHAPTER ROADMAP

By the end of this chapter, readers should be able to (LO1) distinguish measurable risk, ambiguity, uncertainty, vulnerability, crisis, continuity, and resilience, including their philosophical and methodological implications; (LO2) critically compare ERM, high-reliability, contingency, and dynamic-

resilience theories and identify their boundary conditions; (LO3) construct a proportionate governance system with risk appetite, accountable ownership, independent challenge, escalation, and assurance; (LO4) identify and assess strategic, financial, operational, digital, people-related, legal, and systemic exposures using transparent criteria; (LO5) reproduce scenario, expected-loss, liquidity-stress, and sensitivity calculations while recognizing the limitations of numerical risk scores; (LO6) conduct a business impact analysis, specify defensible recovery objectives, and prepare a coordinated crisis and continuity plan; (LO7) appraise Rwandan enterprise vulnerabilities against authoritative international standards and comparable practices; and (LO8) defend a resilience investment and recovery-learning programme that explicitly protects critical stakeholders and tests its own effectiveness.

The chapter moves from conceptual and theoretical foundations (32.0–32.1) to risk accountability (32.2), substantive exposure categories (32.3–32.7), assessment and decision instruments (32.8), continuity and crisis response (32.9), resilience-building and systemic interdependence (32.10–32.11), and recovery and learning (32.12). An extended Rwanda-centred case, international comparison, integrative discussion, research agenda, synthesis, glossary, educational exercises, further reading, and references follow. The analysis builds on Chapter 8's governance principles, Chapter 19's supply-network architecture, Chapter 24's finance, Chapters 28–29's digital foundations, and Chapter 31's sustainability analysis, while preserving those chapters' specialist ownership of their respective topics. It provides a risk-resilience foundation for the subsequent consideration of business ethics in Chapter 33 and enterprise-wide integration in Chapter 35.

32.0 INTRODUCTION: THE ENTERPRISE AS A NETWORK OF VULNERABLE COMMITMENTS

Consider an otherwise solvent wholesale distributor serving retailers and institutions around Kigali. Its customer orders are recorded in a cloud platform, most receipts depend on digital payment channels, two principal suppliers bring goods from outside the city, and dispatch relies on one vehicle and a contracted transport provider. On the same morning, the payment interface becomes unavailable, a main transport corridor is blocked, and the contracted supplier advises that its inventory will be delayed. Sales personnel can still communicate with customers, but cannot confidently promise delivery dates or confirm payments. Accounting sees cash-flow pressure; procurement sees an uncertain replenishment date; employees receive conflicting instructions; and customer-service staff are asked to reassure customers without an authorized account of the situation. None of the three disturbances necessarily destroys the business. Their combination can do so if managerial decisions, information and liquidity fail at the interfaces between functions. This is an explicitly hypothetical teaching situation, not a report of an incident at a named Rwandan firm.

The example illustrates why enterprise risk management is a substantive field of business management rather than a compliance form or isolated insurance task. An enterprise coordinates promises about products, wages, payment, safety, quality, delivery and stewardship through assets and relationships that are only partly under its control. A risk may arise within a function but its effects travel across others: a cyber incident can delay invoicing, reduce collections, interrupt procurement, create employment insecurity and damage trust; a transport disruption can turn viable stock into a working-capital constraint; an ethical breach can affect lending and workforce retention. The managerial challenge is to choose which uncertainties to accept, which to reduce, which to share and which cannot legitimately be imposed upon others (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2017; International Organization for Standardization [ISO], 2018; Organisation for Economic Co-operation and Development [OECD], 2023).

The scholarly challenge is more demanding. Forecastable variation is not the same as radical uncertainty; a risk matrix cannot establish the probability of an unprecedented compound event; and a

firm that survives a shock is not necessarily well governed. Survival may reflect good preparation, external assistance, favourable timing, market power or chance. Conversely, a disciplined organization may suffer an event beyond its reasonable ability to prevent. Decision quality must therefore be judged both ex ante, by the reasons and information available when action was chosen, and ex post, by observed consequences and evidence of learning. March and Shapira (1987), Aven (2016), and Bromiley et al. (2015) provide complementary reasons not to treat either managerial intuition or numerical models as self-sufficient proof.

32.0.1 Evidence design, source hierarchy, and inferential limits

This is a critical, theory-informed documentary synthesis and worked educational analysis, not a systematic review, primary field study, or statistical test of a new model. Sources were selected purposively to cover competing risk and resilience theories, technical and governance guidance, peer-reviewed methodological critiques, and official Rwanda-specific evidence. Preference is given to original academic contributions, current issuing-body documentation, national statistical authorities, and enacted laws. Technical prescriptions are differentiated from voluntary standards; survey estimates from firm-specific measures; and illustrative calculations from observed evidence. The documentary cut-off is 3 November 2026. A complete bibliography supplies traceable source titles, persistent identifiers where confirmed, and institutional links for verification.

The documentary appraisal followed a deliberately limited, reproducible logic. The approved chapter architecture defined the subject boundaries; foundational works were selected to represent competing explanations of probability, organizational accidents, high reliability, risk governance, dynamic resilience and continuity; and institutional documents were checked against the issuing organizations for title, version, legal status and applicability as of the stated cut-off. Rwanda-based material was selected from official statistical, legal and governmental sources, with attention to reference periods, denominators and the difference between a public policy commitment and a measured result. International evidence was included only where the relevant mechanism and source provenance could be stated. Claims were appraised according to source authority, conceptual relevance, temporal fit, independence of evidence, contextual transferability and consistency with the chapter's worked calculations. This is a transparent selection rationale rather than an assertion of exhaustive database coverage, systematic screening counts or primary empirical validation.

The approach supports conceptual comparison, internal consistency checking, explicit assumptions, and a reproducible numerical demonstration. It cannot identify the causal effect of ERM implementation on Rwandan firm survival, infer enterprise-level payment failures from national payment statistics, or estimate actual disruption probabilities without suitably representative exposure and loss data. Those boundaries are not weaknesses to conceal; they define which claims this chapter can responsibly defend. The worked case supplies a decision protocol rather than an estimate of what any particular organization actually did or would earn.

32.1 RISK, UNCERTAINTY, AND RESILIENCE

32.1.1 Intellectual origins and competing concepts

Risk has long been discussed in economics, probability, insurance, safety science and organizational studies, but these disciplines do not define their objects identically. A classical distinction associates risk with settings in which probabilities can be specified and uncertainty with circumstances in which they cannot be established reliably (Knight, 1921). Decision theory sometimes models risk through a distribution of possible outcomes, whereas organizational researchers have shown that managers focus on aspiration thresholds, adverse outcomes and survival constraints rather than solely on expected value and

variance (March & Shapira, 1987). In contemporary risk science, Aven (2016) advocates attention to what is known, what remains uncertain and the strength of the knowledge supporting an assessment. These positions are not merely terminological: they change the information that a decision-maker needs and the level of confidence that a quantitative result deserves.

ISO 31000:2018 defines risk through the effect of uncertainty on objectives, which accommodates both adverse consequences and favourable departures from expectations (ISO, 2018). A hazard is a potential source of harm; exposure refers to the people, assets or activities that could be affected; vulnerability concerns susceptibility and response limitations; and consequence refers to the result if an event or condition affects an objective. An uncertainty becomes managerially relevant when its pathways to objectives, obligations or affected parties can be articulated. The distinction is illustrated by an unreliable transport corridor: flooding is a hazard, delivery dependency creates exposure, absence of an alternative route increases vulnerability, delayed fulfilment is a consequence, and the broader risk depends on conditions of occurrence, impact and knowledge. An opportunity, such as entering a growing market, can be desirable while remaining uncertain; it must not be described as automatically positive for every stakeholder (Hillson, 2002).

Resilience is related but not identical to risk control. Holling's (1973) ecological argument distinguished persistence under disturbance from narrow stability around a single equilibrium. In organizations, Duchek (2020) conceptualizes resilience through anticipation, coping and adaptation; in supply chains, Ponomarov and Holcomb (2009) emphasize readiness, response and recovery. These ideas shift attention from predicting isolated events to retaining function when prediction fails. Yet their intellectual transfer must be qualified: an enterprise is a socially constituted organization with legal obligations and unequal stakeholders, not an ecosystem whose persistence automatically carries moral value. A firm can remain commercially resilient by shifting unacceptable loss to suppliers, employees or communities. Consequently, the socially relevant question is not only whether the organization endured, but what it preserved, at whose cost, through which legitimate processes and with what longer-term effects.

32.1.2 Risk appetite, capacity, tolerance, and residual exposure

Risk capacity is the maximum exposure an organization can absorb before violating survival constraints, capital obligations or other non-negotiable duties. Risk appetite expresses the type and degree of risk it is prepared to take in pursuing objectives; tolerance operationalizes acceptable variation around a particular performance target. A food distributor may accept monthly sales volatility but not unsafe handling of products, deliberately unreported data breaches or inability to meet payroll. A board's appetite statement is ineffective if it says merely that risk should be low. It must be translated into measurable limits, such as a minimum cash buffer, maximum customer concentration, recovery objectives for essential activities, and unambiguous escalation rules. The distinction between capacity and appetite also matters: having the cash to bear a loss does not make the conduct that creates the loss ethical or lawful (COSO, 2017; OECD, 2023).

Inherent risk denotes exposure considered before specified treatments; residual risk describes the exposure remaining after those treatments operate. Neither quantity is directly observable without a clearly defined reference scenario. Controls can introduce new dependencies: moving all information to one cloud provider may reduce risks from lost paper records while increasing common-cause outages. Managers should record control assumptions, evidence of operating effectiveness, and the treatment-induced risks rather than treating residual scores as objective facts. Risk acceptance is an explicit decision by an accountable person, informed by available evidence and bounded by legal and ethical constraints; it is not permission to ignore risk. Risk transfer through insurance, outsourcing or contracts rarely transfers every reputational, operational or moral consequence.

32.1.3 From risk events to dependency networks

In a functional organization, a risk register often lists incidents by departmental owner. The same event may then appear repeatedly, while a shared dependency is invisible. A more defensible model begins with value-critical outcomes and traces the activities, people, suppliers, data, payments and infrastructure on which each depends. Figure 32.1 represents the enterprise as a set of reciprocal commitments where a disturbance can propagate through different pathways. A risk assessment should specify initiating condition, transmission mechanism, affected objective, vulnerable interface, safeguards, plausible consequence, and evidence quality. This account is compatible with ISO 31000, but adds an explicit organizational-dependency interpretation rather than claiming that the diagram is an issued standard or empirically validated tool.

32.1.4 Competing explanations of organizational failure and adaptation

A satisfactory theoretical account must explain both the occurrence of disruption and the capacity to maintain legitimate function despite it. Expected-utility models offer a coherent choice rule when outcomes, probabilities, preferences and relevant constraints can be represented with sufficient validity. Their explanatory strength is the explicit comparison of uncertain alternatives. Their limitation is epistemic: a highly precise probability for a novel interconnected disruption may be an expression of confidence rather than a measurement. Knightian uncertainty and Aven's (2016) knowledge-sensitive perspective therefore make the grounds for belief part of the decision itself. Two managers may agree on a projected loss but disagree legitimately about the credibility of the scenario distribution, and risk governance must disclose that disagreement rather than average it away.

High-reliability and normal-accident perspectives point toward a more structural disagreement. The high-reliability tradition studies how demanding organizations can maintain unusually dependable performance through operational attention, learning from weak signals and the authority of situated expertise (Weick & Sutcliffe, 2015). Perrow's (1984) normal-accident reasoning, by contrast, emphasizes that tightly coupled, interactively complex technologies can produce combinations of failure that cannot all be anticipated or prevented. The literature review by Cantu et al. (2020) identifies the prominence of culture in high-reliability scholarship, but its synthesis does not show that the same practices invariably prevent serious incidents across sectors. These arguments are not logically incompatible. Attentiveness can reduce some vulnerabilities while tight coupling preserves residual pathways to unanticipated failure. The governance question is thus when simplification, decoupling or exit from a dangerous activity is more defensible than another layer of monitoring.

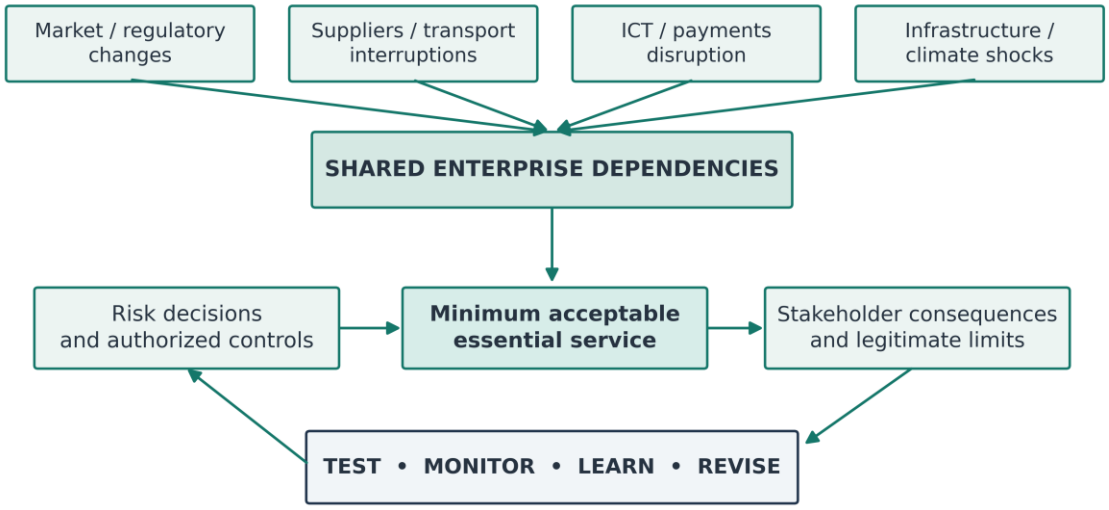
A third account interprets resilience as an organizational capability developed through anticipation, coping and adaptation rather than as a fixed reserve of assets (Duchek, 2020). Bhamra et al. (2011) similarly highlight the interfaces between organizations and enabling infrastructure, while Lengnick-Hall et al. (2011) develop the argument that employee cognition, behaviour and contextual conditions contribute to resilient responses. These studies broaden the unit of analysis beyond the asset or incident, but capability language can become circular if firms are called resilient simply because they recovered and then said to have recovered because they possessed resilience. Empirical tests must therefore measure the proposed antecedents independently of the outcome: for example, independently confirmed alternate-provider availability, observed drill performance, cross-trained decision authority and prior liquidity coverage.

Institutional and ethical approaches add a fourth, indispensable dimension. A business can survive by delaying small suppliers, shifting unsafe work to subcontractors or using dominant contractual power to secure scarce goods. A purely firm-centred resilience measure might report success while the wider network becomes more fragile. The proposed analytical synthesis therefore distinguishes *private persistence*, *legitimate service continuity* and *system-level resilience*. Their relations depend on market

power, public infrastructure, enforceable rights and the distribution of adjustment costs. The implication is not that enterprise continuity should cease to matter, but that its desirability must be defended in relation to what continues, who is protected and what burdens are transferred (OECD, 2023; Bhamra et al., 2011).

Figure 32.1

Cross-functional propagation and resilience decision loop.



Note. Original conceptual synthesis informed by ISO (2018), Duchek (2020), and Christopher and Peck (2004). Arrows represent hypothesized dependencies requiring organization-specific validation, not estimated causal effects.

32.2 RISK GOVERNANCE AND ACCOUNTABILITY

32.2.1 The legitimacy of risk authority

Effective ERM begins with a question of authority: who may expose the enterprise and its stakeholders to a consequential possibility of harm, and what makes that choice legitimate? Governing bodies authorize purpose, strategic direction and broad limits; executives allocate resources and establish procedures; operational managers own decisions and controls; specialist functions provide challenge and coordination; and internal auditors can provide independent assurance within the scope of their mandate. Governance should make disagreement possible before a crisis, because reassurance conveyed upward may otherwise conceal vulnerability. The G20/OECD Principles of Corporate Governance place particular emphasis on board oversight of risk and the integrity of reporting and control arrangements (OECD, 2023). This does not imply that a small enterprise requires the committees and headcount of a listed bank; it requires a proportional allocation of duties that remains intelligible and reviewable.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) revised its enterprise risk framework in 2017 to embed risk thinking within governance, strategy and performance, rather than adding an inventory at the end of planning (COSO, 2017). ISO 31000:2018 similarly distinguishes principles, an organizational framework and the iterative process of communication, scope-setting, assessment, treatment, monitoring and recording (ISO, 2018). COSO is a conceptual management framework; ISO 31000 is voluntary guidance and explicitly not a certifiable management-system standard. Neither document, by itself, creates a statutory obligation in Rwanda. Legal obligations must instead be traced to applicable laws, regulators, contracts and sector-specific instruments.

32.2.2 Three Lines, independence, and proportionality

The Institute of Internal Auditors (IIA) issued two distinct Statements of Position on 8 July 2026: *Three Lines Model: Assurance and Advice in Support of Effective Governance* and *The Role of the Internal Audit Function in Enterprise Risk Management*. The refreshed statements emphasize governing-body accountability, management ownership, coordinated advisory and assurance contributions, and the independence of internal audit where it performs third-line work (IIA, 2026a, 2026b). The older language of three impenetrable defensive barriers is misleading: risk information must move rapidly across functions, while auditors must not become the decision-makers whose work they later purport to assure. Where a chief audit executive undertakes second-line activities, explicit safeguards are necessary. A single-person enterprise cannot produce structural independence internally; it can nonetheless document risk acceptance, obtain periodic external review, and establish transparent alternative checks proportionate to its resources.

Table 32.1

Governance responsibilities for enterprise risk and continuity

Accountability level	Core decision rights	Evidence and safeguards	Escalation boundary
Governing body or owner	Approve objectives, appetite, crisis authority and resources	Risk-appetite record, critical-service review, challenge minutes	Threat to survival, rights, regulatory duties or essential services
Executive management	Integrate risk into strategy, budgets and response priorities	Consolidated scenarios, business impact analysis, crisis delegation	Breach of limits, persistent gaps or conflicting function priorities
Operational risk owner	Identify exposure, operate treatment, report incidents	Control logs, supplier tests, verified recovery evidence	Control failure or consequence outside delegated authority
Specialist risk, legal, safety and ICT roles	Set method, challenge assumptions and advise on obligations	Independent checks, exceptions, documented opinions	Material unaddressed deficiencies or legal uncertainty
Internal audit or independent reviewer	Provide appropriately independent assurance	Risk-based assurance work and limitations	Unresolved material control and governance failures

Note. Original adaptation informed by COSO (2017), OECD (2023), and IIA (2026); roles may be combined in smaller entities, but incompatible authorization and assurance responsibilities should be disclosed.

32.2.3 Designing a workable governance cycle

A usable governance cycle links an annual review of strategic assumptions to quarterly examination of critical dependencies, immediate incident escalation and periodic assurance on whether selected controls function as designed. Each material risk needs a named decision owner and an operational control owner, even where both roles sit with one individual. A well-maintained record specifies the objective, scenario, source of exposure, present safeguards, evidence confidence, tolerance, planned action, funding, residual uncertainty, review date and escalation trigger. Risk committees should spend more time challenging consequential assumptions and trade-offs than rearranging colours on a heat map. When incentives reward uninterrupted growth or apparently perfect compliance, staff may hide near misses; psychologically safe reporting and documented corrective decisions are part of effective governance, not optional culture programmes (Mikes, 2009; Weick, 1988).

32.2.4 Risk appetite, incentive conflicts, and credible challenge

Risk appetite is most useful when translated into decisions that could otherwise be contested. Management may accept price volatility to enter a regional market while insisting that the same expansion never bypass product-safety requirements or create a foreseeable inability to pay employees. A defensible appetite statement therefore has three layers: the enterprise's strategic willingness to assume uncertainty, operational limits at which authority must be escalated, and binding legal and ethical boundaries that cannot be relaxed by economic calculation. The latter are not merely another category of low-tolerance risk. They are constraints on permissible choice. When an organization treats potential legal penalties as the full cost of foreseeable harm, its model omits the claims of those exposed to the harm.

Governance arrangements must also confront incentive incompatibility. A sales director rewarded for quarterly volume may favour customers with weak credit; procurement rewarded only for purchase-price savings may understate supplier fragility; technology leaders evaluated by implementation dates may postpone migration testing. Reporting these exposures separately creates the appearance of local success even as the enterprise accumulates correlated downside. A practical response links the governing body's critical-service and liquidity limits to each function's performance measures, and requires material exceptions to be jointly signed off by finance, operational management and the designated risk owner. Independent internal audit, where available, evaluates the design and operation of these arrangements rather than becoming the author of the commercial decisions (IIA, 2026a, 2026b).

The quality of challenge depends as much on evidence and power as on charts and committees. An owner-managed firm may substitute a periodic review by an external accountant and a documented challenge from a principal supplier for a formal risk committee, provided scope, competence and conflicts are understood. A larger company may have extensive assurance teams yet fail to correct repeated warnings when executives can suppress escalation. Accordingly, a useful governance evaluation asks not whether the organization possesses a particular title or committee but whether consequential assumptions can be questioned, material breaches reach an authorized decision-maker, corrective resources can be released and recorded exceptions are independently retested (Mikes, 2009; Bromiley et al., 2015).

32.3 STRATEGIC AND MARKET RISKS

Strategic risk arises when chosen objectives, business models and capability commitments become inappropriate because critical assumptions are false, competitors act differently, customers change, or institutions alter the feasible set of transactions. Market demand can contract while input commitments remain fixed; a new platform may change price transparency; policy reforms can affect licensing, product eligibility or export access. Strategic opportunity and strategic risk are inseparable because an organization may reasonably accept uncertainty to obtain a valued outcome. Kaplan and Mikes (2012) distinguish preventable internal risks, risk voluntarily assumed by strategy, and external risks requiring different governing responses. Their typology is pedagogically useful but not mutually exclusive in practice: a deliberate concentration strategy can increase exposure to an external supplier failure, and poor internal oversight can amplify a market decline.

The analytic task is to test the strategy's *conditions for success*. A responsible strategy record specifies assumptions about demand, contribution, customer concentration, supplier access, affordability, competitor behaviour, operating permission, managerial capacity and liquidity. Early-warning indicators must correspond to causal channels rather than simply repeat lagging revenue. For a Rwanda-based enterprise selling into neighbouring markets, customer-order cancellations may be more informative than national GDP growth; a dependent importer may need corridor and exchange-rate indicators alongside sales; and a business serving institutions should monitor payment timing as well as contract awards. Scenario planning can compare a baseline, gradual deterioration and an abrupt structural shift, but stories

are not probabilities unless supported by a justified forecasting design. Chapter 6 established competitive analysis; the present chapter asks how strategic commitments can fail and how management should adapt without arbitrary retrenchment.

Reputational risk requires particular care. Reputation is not an independent substance that can be insured against all criticism; it is a relational assessment produced by conduct, customer experience, disclosures, social narratives and the perceived fairness of remedies. The distinction matters when a company labels legitimate worker complaints or public criticism as a risk to suppress rather than as evidence of an unresolved obligation. A credible response tests the factual basis of claims, protects lawful speech and whistleblowing, corrects failures and communicates uncertainty honestly. Strategic risk governance is therefore inseparable from the epistemic quality and legitimacy of managerial decisions, though the full normative comparison of ethical theories is retained for Chapter 33.

32.3.1 Demand, concentration, and competitive discontinuity

Market risk is frequently assessed through the volatility of revenue, but the enterprise's exposure arises from the commitments made on the expectation that revenue will materialize. A wholesaler with short-term inventory, variable labour and readily transferable logistics capacity can absorb a demand reduction differently from a manufacturer with specialist machinery, binding debt service and a small number of customers. A strategic risk analysis therefore joins the demand-side question, *how much business might disappear?*, to the supply-side question, *how quickly can the organization change its cost and asset commitments without harming others or breaching obligations?* The interaction creates asymmetry: sales may decline immediately while costs adjust only after contracts or retraining periods.

Concentration requires careful denominator choices. A customer supplying 40% of annual sales may account for a larger or smaller share of contribution, receivables or expected future growth. Similarly, a supplier's share of purchase value does not reveal its irreplaceability when it supplies an inexpensive but indispensable component. Decision-grade concentration analysis therefore distinguishes sales share, contribution share, debtor exposure, substitutability, contractual exit costs and network common causes. Diversification should not be presumed beneficial simply because it increases the number of names on a supplier register; if the substitute raises costs without reducing a common bottleneck, the apparent improvement may be illusory. These distinctions connect strategy to credit management and the operational network without repeating the specialist methods developed in Chapters 6, 19 and 24.

32.3.2 Policy transitions, reputation, and strategic reversal

Regulatory or policy change is not only a compliance risk after legislation takes effect. The anticipation of proposed measures may reshape customer expectations, finance terms, product design and investment decisions. Nonetheless, consultation drafts, enacted statutes, administrative circulars and public commitments possess different legal authority. A strategy team should maintain a dated policy-source register, identify specific affected transactions, model alternatives and obtain jurisdictional advice where uncertainty is consequential. Treating a speculative announcement as enforceable law is as indefensible as ignoring an enacted prohibition. The assessment must also recognize that political and administrative risks may be distributed unevenly across enterprise types, locations and ownership models.

A strategic reverse stress test turns the question from *What is our expected growth?* to *Which plausible combination of customer loss, financing pressure and delayed adaptation would make our chosen strategy unacceptable?* Consider a proposed regional expansion that requires upfront inventory and a single foreign-currency collection channel. A severe demand reduction may have little impact if the enterprise can quickly cancel replenishment and preserve cash. It becomes existential when receivables are delayed, the inventory is specialized and a refinancing date falls within the same quarter. A credible board memorandum compares abandonment, staged entry and contractual flexibility as distinct decisions, not as

optimistic and pessimistic versions of one forecast. The manager must also assess whether reputation is being protected by remedying actual misconduct or merely by suppressing legitimate criticism (Kaplan & Mikes, 2012; OECD, 2023).

32.4 FINANCIAL AND LIQUIDITY RISKS

Financial risk includes the possibility that expected cash flows, asset values, financing access or contractual settlements depart sufficiently from plan to impair an enterprise's obligations and choices. The main categories are credit or counterparty non-performance, cash-flow mismatch, refinancing pressure, interest-rate sensitivity, foreign-exchange exposure, asset-price movements and contingent obligations. Their mechanisms differ. A profitable enterprise may fail to pay wages when receivables are delayed; a solvent balance sheet may coexist with an immediate settlement shortage; and a cheap foreign-currency loan may become expensive in local-currency terms if the exchange rate moves unfavourably. Financial risk must therefore be assessed across timing, currency, contractual enforceability and liquidity, rather than reduced to projected annual profit (Chapter 24).

Cash stress testing begins with an opening unrestricted cash balance, confirmed inflows, essential unavoidable outflows, contingent costs, committed but undrawn facilities and a minimum survival buffer. The relevant object is the cash path, not merely its closing total: a temporary negative balance may invalidate an otherwise positive month-end projection. A scenario-based cash position at time t can be expressed as $C_t = C_0 + \Sigma$ collections_1..t + Σ committed usable funding_1..t − Σ unavoidable payments_1..t − Σ response costs_1..t. A liquidity gap arises when the minimum projected balance falls below an operationally and contractually justified buffer. The uncertainty attached to every term should be disclosed; a bank line subject to discretionary renewal is not equivalent to cash in hand.

Counterparty concentration creates an interaction among finance, sales and operations. When a single institutional buyer accounts for most receivables, its late payment can delay procurement even if it eventually settles in full. Exposure measurement should distinguish gross invoiced amounts, expected recoveries, contractual security and correlated counterparties. Foreign-currency risks should distinguish transaction exposure from the economic effect of imported inputs becoming less affordable; presenting a formula for hedging without transaction volumes, available instruments, counterparty costs and local market constraints would be false precision. Insurance and trade finance may mitigate certain losses but impose premiums, exclusions, collateral and documentation requirements. Detailed valuation, interest-rate mathematics and investment decisions remain in Chapter 24; the present emphasis is functional interdependence and the continuity consequences of financial constraint.

At a systemic level, reliable payment infrastructure is essential to commerce, but national statistics must not be misrepresented. The National Bank of Rwanda (NBR) describes payment-system stability in its 2024/25 reporting without major interruptions in the reporting period and reports substantial expansion in mobile payments (NBR, 2025). A hypothetical outage in a teaching case is consequently not evidence that such a national outage happened. It illustrates why firms dependent on any external settlement pathway should agree a lawful offline or alternate arrangement, preserve transaction evidence, protect customers against duplicate payments, and decide who has authority to release goods while settlement remains uncertain.

32.4.1 Funding liquidity, market liquidity, and temporal solvency

Liquidity and solvency require different evidence. Accounting assets may exceed liabilities while the enterprise lacks immediately usable funds to meet obligations on their due dates. Conversely, a company can hold abundant temporary cash despite an unsustainable business model whose future obligations exceed its earning capacity. Financing facilities are conditional claims rather than perfect substitutes for

cash: drawing may depend on covenant compliance, collateral valuation, bank operating hours, counterparty availability or the continued operation of payment systems. An adequately designed stress test therefore records the legal and practical availability of each source of funds, not merely its nominal limit.

Consider an expressly illustrative importer that owes USD 20,000 for goods and has not hedged the payment. If the decision model assumes an exchange rate of RWF 1,450 per dollar, the invoice requires RWF 29,000,000. An adverse 8% increase in the local-currency cost of a dollar raises the assumed outflow to RWF 31,320,000, an additional RWF 2,320,000 before fees. These are invented input values, not historical exchange-rate observations. Their educational value is that a foreign-currency shock can reduce procurement capacity and liquidity even if selling prices have not changed. The relevant response may combine price review, shorter payment periods, partial currency matching and purchasing flexibility; each requires examination of customer demand, contract conditions, hedge availability and distributional effects rather than a claim that hedging is universally accessible.

32.4.2 Liquidity risk as a constraint on resilience investment

An important paradox follows. A continuity option can lower the expected total cost of a disruption while worsening cash shortages in the first hours of the event. Emergency freight, substitute technology, upfront supplier deposits and temporary accommodation can require payment before the avoided revenue is collected. Finance must therefore test the *peak cumulative cash deficit* under a daily or finer time grid, with particular attention to payroll, debt service, tax obligations and emergency expenditure. An end-of-period positive cash number does not eliminate the need for bridge finance within the period. A robust decision compares options not only by expected loss but by minimum cash, financing certainty, earliest breach of a survival threshold and the social consequences of each financing arrangement.

Insurance analysis follows the same discipline. A policy can reduce specified financial consequences but cannot itself reopen a road, prevent injury or guarantee a provider's performance. Its usefulness depends on scope, deductibles, exclusions, waiting periods, claims evidence, counterparty strength and the time until a claim is paid. In a compound event, a manager should not record hypothetical insurance recovery as available operating cash unless the trigger, coverage and receipt timing are sufficiently supported. This is particularly consequential in smaller enterprises where a profitable insurance claim months later cannot resolve immediate payroll and supplier-payment pressures (Aven, 2016; COSO, 2017).

32.5 OPERATIONAL AND SUPPLY-CHAIN RISKS

Operational exposure arises through the activities, resources and interfaces required to deliver products and services. It includes process error, equipment breakdown, quality failure, deficient maintenance, inventory discrepancies, safety incidents, utility interruption, insufficient skills and flawed handoffs. Supply networks extend this exposure beyond the organization’s formal boundary to suppliers, transport operators, ports, digital platforms, regulators and customers. Traditional efficiency programmes can reduce direct cost while simultaneously removing inventories, alternative suppliers and spare capacity that would buffer shocks. Christopher and Peck (2004) and Sheffi and Rice (2005) show why resilience considerations are integral to operating-system design rather than merely a contingency added after optimization.

A systematic diagnosis follows a critical offering backwards from customer receipt to physical and informational prerequisites. It identifies whether any component has a single source, whether alternative suppliers are genuinely independent, what contractual lead times and standards apply, and whether substitute logistics routes remain feasible under a shared regional shock. A backup supplier using the same border, sub-supplier or payment service may create the illusion of diversification without reducing

common-cause exposure. The relevant unit of analysis is therefore a dependency network, not only a supplier list. Procurement ownership remains in Chapter 18, inventory policy in Chapter 19 and quality-method detail in Chapter 20; enterprise risk oversight concerns how these choices interact under disturbance.

The operational consequences of delay are nonlinear. A four-hour interruption might be absorbed by scheduled capacity; once an order deadline passes, the same interruption can trigger penalty, spoilage, lost customer orders or cascading rework. Staff may compensate by rushing, creating a secondary safety or quality risk. Managers should distinguish prevention controls (inspection, maintenance, access restrictions), detection controls (reconciliation, alarms, exception reporting), response controls (workarounds and escalation), and recovery controls (verified restoration). Each control should have a testable outcome and a failure mode. In smaller Rwandan businesses, documentation can be concise: an updated supplier contact sheet, manual stock record, alternative payment arrangement and customer-notification procedure may generate more defensible benefit than an untested, expensive system (Herbane, 2010).

32.5.1 Propagation, substitution, and operating thresholds

A supply chain can be mapped as a directed network of activities with multiple forms of dependence: physical input, transport access, information, payment and contractual authority. The network perspective exposes why the apparent independence of two providers may not survive a shared shock. Two transport companies might use the same flooded corridor; two digital platforms might use one cloud identity service; two suppliers might rely on a common imported raw material. A meaningful alternative is one whose critical failure points are sufficiently independent under the particular scenario. Testing that claim requires more than collecting supplier assurances: the enterprise should inspect relevant routes, lower-tier dependencies, lead-time variability, permission to substitute and the actual time required to activate the alternative (Christopher & Peck, 2004; Jüttner et al., 2003).

Operational resilience should be evaluated as *time-dependent service*, not only production recovered at the end of the month. Different customers may tolerate different interruptions; a hospital's emergency supplies, a school's meal programme and a retailer's routine replenishment do not have identical consequence profiles. For each priority service, managers should identify an acceptable minimum, a trigger for unacceptable degradation and a verifiable safe resumption test. Recovery decisions must include product integrity and worker safety: goods exposed to inappropriate conditions should not be dispatched merely to restore a delivery percentage, and staffing shortages should not be resolved through unsafe overtime. When safe minimum service cannot be delivered, a controlled suspension with transparent notice may be the most responsible continuity action.

32.5.2 Working capital, infrastructure, and contractual remedies

A disruption changes the economics of inventory. Buffer stock can protect sales but ties up cash and may deteriorate; low stock can improve normal-period efficiency while making a short road closure catastrophic. These are trade-offs rather than universal defects. An enterprise should compare alternative stock, supplier and transport policies on total relevant cost, the time profile of service, common-cause exposure and financing needs. A supplier's contractual service-level commitment should be examined alongside feasibility, escalation contacts, substitution rights, force-majeure terms and the practical remedy available when many buyers are affected simultaneously. A damages clause does not deliver food, medicines or spare parts during an interruption.

In Rwanda and other landlocked settings, public infrastructure creates dependencies that private contracting alone cannot eliminate. The relevant continuity plan may need corridor monitoring, alternative shipment timing, communication with local authorities and transparent postponement arrangements. It

must distinguish a documented public disruption from conjecture about its likelihood at a particular site. Managers should also record whether an alternative logistics route increases emissions, road-safety exposure or burdens on nearby communities. This is not an argument against resilience investment; it is an argument for evaluating what the investment actually protects and what additional costs it imposes (Bhamra et al., 2011; United Nations Office for Disaster Risk Reduction [UNDRR], 2015).

32.6 TECHNOLOGY AND INFORMATION RISKS

Information systems coordinate sales, payments, logistics, accounting, human resources and regulatory records. Their failure can therefore be systemic even when the initiating defect is technical. The relevant threat landscape includes malicious intrusion, credential compromise, software errors, corrupted or unavailable data, cloud and telecommunications outages, weak integration, insecure third-party access, algorithmic mistakes and difficult-to-exit provider arrangements. Confidentiality, integrity and availability are analytically distinct: an enterprise may continue to receive orders while customer records are exposed, or possess intact data that staff cannot access when required. The NIST Cybersecurity Framework 2.0 organizes high-level outcomes into Govern, Identify, Protect, Detect, Respond and Recover; its functions support managerial coordination but do not guarantee that a specified security product or control will work (Pascoe et al., 2024).

Rwanda's National Cybersecurity Strategy 2024–2029 identifies cyber resilience and trust, domestic cybersecurity capability, and cooperation as strategic priorities (NCSA, 2024). Its objectives are public policy commitments, not proof that every enterprise has equivalent technical maturity. Rwanda's Law No. 058/2021 concerning personal data and privacy creates substantive data-governance obligations, whose applicability and detailed compliance should be checked against the enacted text and regulator guidance for the specific processing activity (Republic of Rwanda, 2021). A digital continuity plan should therefore combine secure backups, restoration tests, identity and access control, incident evidence preservation, service-provider escalation, privacy compliance, and transparent customer communication. Backups are inadequate if they cannot be restored, if encryption keys are lost, or if backup copies share the same compromised administrative account.

Artificial intelligence adds model and decision risks beyond traditional software failure: distribution drift, inappropriate automation, fabricated outputs, insufficient monitoring, privacy exposure and confusion over human responsibility. These risks matter to ERM insofar as they threaten enterprise objectives and other functions; model-validation metrics and AI-specific controls remain principally within Chapter 29. A manager should ask which decisions an AI service influences, what human contestation is possible, whether a model failure would propagate to multiple processes, and how the enterprise can operate safely without the service. For critical decisions, an alternate manual pathway may be a resilience control as consequential as cyber defence itself. Vendor lock-in should also be assessed against migration time, exportable data formats, service-level terms and the concentration of both data and operational expertise.

32.6.1 Security, recoverability, and the integrity of manual workarounds

Cybersecurity and business continuity can reinforce one another, but their objectives are not identical. Access controls and network isolation can prevent unauthorized transactions, while a recovery team may require rapid access to essential records. Emergency access therefore needs preauthorized limits, individual attribution, an expiration mechanism and independent post-event review. A manual payment or customer-order workaround is not inherently safer than an automated process; it can create transcription errors, duplicate settlement, leaked personal information and unauthorized credit. Equally, a technically secure system that remains unavailable for days may be incapable of supporting essential contractual

commitments. The appropriate design separates prevention, controlled fallback, evidence retention and verified reconciliation.

Recovery objectives must distinguish availability from integrity. A backup may restore quickly but contain contaminated or incomplete data. The enterprise should specify the source of truth for orders, receipts, stock and customer contact information and demonstrate its ability to reconcile records captured through separate channels. Where the service provider is external, a signed service-level agreement is useful evidence of contractual expectation, not proof of actual recovery capability. Test design should include identity-provider unavailability, loss of internet connectivity, inability to decrypt a backup and incompatible software restoration. This reasoning extends the digital architecture in Chapter 28 without duplicating its technical configuration details (Pascoe et al., 2024; ISO, 2019).

32.6.2 Algorithmic dependencies and the right to contest

AI-assisted demand forecasts, fraud screening, recruitment and customer support may appear to diversify managerial capacity but can also create a shared dependence on one model, dataset or provider. A generative service that returns plausible yet false customer instructions can worsen a crisis precisely when staff are under pressure and verification is difficult. A resilience-oriented AI governance programme therefore identifies decisions whose outputs require validation, distinguishes advisory from autonomous action, defines human override authority and tests safe operation when the model is disconnected. High prediction accuracy in ordinary records does not establish reliability after a shock that changes the underlying distribution of events.

The ethical issue is not simply model error. Automated procedures can distribute delay, credit denial or access to scarce resources unequally, while the persons affected may lack an intelligible explanation or remedy. Risk governance should therefore preserve documentation of decision criteria, a practical review channel and accountability for adverse effects. For high-consequence decisions, a human reviewer must have the competence, information and genuine authority to disagree with the system, rather than providing a ceremonial approval. Formal model evaluation belongs to Chapter 29; the ERM question is whether the enterprise can maintain lawful, explainable decisions without the technology and can detect the systemic consequences of its failure.

32.7 PEOPLE, LEGAL, AND CONDUCT RISKS

Human beings are simultaneously an enterprise's principal source of judgment, skill, relationships and adaptive capacity, and people who can be harmed by organizational decisions. A people-related risk is not adequately expressed by "key employee unavailable" or "staff error." The analyst should distinguish hazardous working conditions, under-resourcing, excessive workload, discriminatory treatment, inadequate training, deficient supervision, concentration of tacit knowledge, employee departures and failures of organizational voice. An enterprise that relies on unpaid overtime as its only recovery mechanism may preserve deliveries temporarily while creating injury, attrition, fatigue and further control failures. Consequently, resilience evaluation must examine the distribution of recovery burdens as well as aggregate service levels. Employment rights and detailed statutory workplace standards remain the concern of Chapter 11, while the risk chapter concentrates on how people-related vulnerabilities affect enterprise continuity.

Legal risk includes noncompliance with binding statutes and regulations, defective contractual terms, exposure to litigation, uncertain interpretations and unenforceable commitments. Conduct risk includes fraud, bribery, misleading sales, misuse of confidential information, retaliation against reporting staff and improper responses to crises. Some exposures require prevention and reporting rather than a calculated trade-off: a manager cannot ethically authorize a known unsafe practice simply because its expected fine

appears cheaper than safe operation. Legal consequences vary by jurisdiction, type of enterprise and regulated activity; no generic checklist replaces a source-specific compliance register maintained with qualified advice where needed. An organization trading across borders may also encounter conflicting requirements on privacy, consumer safeguards, product claims or employment. Chapter 3 established the institutional context and Chapter 26 developed financial compliance and assurance; here the relevant question is how legal and conduct failure can interact with other shocks.

Culture matters to risk because information is imperfect and authority is unequal. Early warnings often begin as ambiguous signals from operators, drivers, cashiers or customers, not as complete statistical reports. An employee who expects blame for reporting a near miss may conceal it; an executive whose bonus depends narrowly on quarterly revenue may dismiss a slow-developing continuity threat. The high-reliability tradition directs attention to weak signals, operational expertise, an informed reluctance to oversimplify, and sensitivity to the processes actually being performed (Weick & Sutcliffe, 2015). The promise of these ideas is disciplined attentiveness. Their limit is that such attentiveness takes resources, can conflict with short-term incentives, and cannot remove structural conditions imposed by poverty, weak infrastructure or coercive power. Resilience therefore requires credible incident-reporting rights, role substitution, safe-work thresholds, accessible grievance channels and clear accountability for breaches, not ceremonial claims of a "risk-aware culture" (Weick, 1988; OECD, 2023).

A practical people-continuity protocol identifies a minimum skill complement for each critical activity, a second authorized operator, contact and substitution procedures, worker-safety requirements, access to personal protective measures where needed, and arrangements for psychosocial support after serious incidents. It should never presume that sensitive health records can be collected or circulated indiscriminately. Before a major staffing decision, management should ask whether a temporary closure or reduced service is preferable to unsafe work, whether customers can receive a transparent revised commitment, and whether emergency subcontracting would violate labour or procurement requirements. In such choices, the welfare of people is an operational constraint and a legitimate outcome, not only a component of financial loss.

32.7.1 The organizational production of human error

A weak risk analysis often treats human error as an initiating cause and stops there. Yet a mistaken dispatch, misapplied payment or missed safety warning may reflect poorly designed work, ambiguous responsibilities, fatigue, unreliable information, impossible targets or a lack of access to operational expertise. Assigning sole blame to the last employee in the transaction conceals the management decisions that created the conditions. Lengnick-Hall et al. (2011) explain resilience partly through the cognitive, behavioural and contextual capacities developed within workforce systems; the implication for ERM is to treat training, role substitution, decision rights and conditions for honest reporting as controls requiring evidence, not as expressions of goodwill.

The distinction between culpable misconduct and reasonable error is also a matter of justice. Fraud and intentional retaliation warrant investigation and proportionate consequences, whereas an employee acting within an unsafe procedure may reveal an institutional defect. Both situations require factual reconstruction, rights of response and protection against arbitrary punishment. Emergency disciplinary shortcuts can destroy the credibility of incident reporting and produce future concealment. This issue connects to Chapter 11 on employment relations and Chapter 8 on accountable governance while keeping the present focus on risk propagation and continuity. During significant crises, a qualified occupational-health or safeguarding adviser may be required, but the absence of an adviser does not justify ignoring evident hazards.

32.7.2 Integrity, fraud, and decision legitimacy under stress

Crisis conditions expand both discretion and opportunity for abuse. Normal authorization chains may be interrupted; urgent purchases can bypass competition; goods may be scarce; and staff may use personal communication channels to maintain contact. A responsible emergency procedure permits necessary speed while preserving evidence. It defines temporary authority limits, separation of requisition and payment where feasible, a list of approved exceptional suppliers, documentation of conflict-of-interest declarations and a timed post-event review. In a very small enterprise, a founder may necessarily authorize both purchase and payment, but independent bank reconciliation and external review can still provide compensating controls (COSO, 2017; OECD, 2023).

Organizations should resist two opposed errors: treating compliance as a document completed before a crisis, and treating urgency as permission to suspend all legal obligations. Notification duties, customer rights, labour protections and data privacy requirements can continue during emergencies, although the applicable legal procedures may provide specific exceptions. A risk team should maintain accessible, dated legal contacts and escalation instructions, while recognizing the limits of its own competence. Where a law or regulator mandates immediate action, ethical and legal duties take priority over the convenience of a probability-weighted business case (Republic of Rwanda, 2021; IIA, 2026a).

32.8 RISK ASSESSMENT TECHNIQUES

32.8.1 From exposure statements to decision-grade evidence

Risk assessment starts by specifying the decision, the relevant objective, an acceptable time horizon and an explicit scenario. Without that foundation, a likelihood score cannot be interpreted. The common process includes establishing criteria, identifying conditions and causal pathways, analysing possible consequences and uncertainties, evaluating exposure against decision thresholds, and selecting treatment with monitoring arrangements (ISO, 2018; IEC, 2019). Evidence may come from records of failures, industry data, expert elicitation, engineering characteristics, contracts, financial accounts, operational tests and stakeholder testimony. Each source has a different selection process and inferential reach. A failure-free history is weak evidence for a low-frequency catastrophic event if the observation window is short or relevant conditions have changed.

A risk register is useful as a structured memory, but not as the risk itself. The strongest entries state a cause and an observable consequence linked to an objective: “Because both payment channels rely on the same service-provider connection, an outage lasting more than eight hours could prevent confirmation of receipts, cause duplicate customer collections and delay dispatch.” By contrast, “payment risk, high” does not identify a testable control or an accountable decision. Table 32.2 illustrates a register suitable for a resource-constrained distributor and is expanded in the Rwanda case. The confidence column is essential: identical numerical scores may be based on documented service history in one row and unsupported managerial judgement in another.

Table 32.2

Integrated risk register for a constructed Rwandan distributor

ID and objective at risk	Trigger and dependency mechanism	Consequence and current safeguard	Owner and response	Monitoring evidence and trigger
R1: timely receipts	Primary digital payment interface unavailable; backup shares telecommunications link	Collections uncertain; manual reconciliation available	Finance lead: independent alternate, receipt verification	Test alternate monthly; escalate at 2 hours

ID and objective at risk	Trigger and dependency mechanism	Consequence and current safeguard	Owner and response	Monitoring evidence and trigger
R2: on-time distribution	Road closure and dependence on one carrier	Delivery delay; limited vehicle flexibility	Operations lead: route and carrier alternatives	Daily corridor status; escalate at 6 hours
R3: product availability	Principal vendor misses two replenishment cycles	Stockout and lost orders; safety stock limited	Procurement lead: prequalify second source	Cover days below six; immediate escalation
R4: cash survival	Combined collection delay and exceptional expenditure	Liquidity below minimum operating buffer	Finance lead: rolling cash stress plan	Daily forecast; escalate at RWF 2m floor
R5: lawful customer records	Offline process creates inaccurate or exposed personal data	Claims, privacy harm, unreliable settlements	ICT/data lead: controlled paper log and access	Exception report and secure destruction schedule
R6: employee and customer safety	Pressure to dispatch through unsafe conditions	Injury or product integrity failure	Director: stop-work authority and safe resumption	Hazard confirmation; immediate stop threshold

Note. All enterprises, events, thresholds and controls in this register are hypothetical. Ratings are not presented because the supporting probability data do not exist. Control effectiveness must be tested, not presumed.

32.8.2 Why heat maps are inadequate as stand-alone decisions

Many organizations convert qualitative labels such as “unlikely” and “severe” into numbers from one to five, multiply them and rank the resulting products. Such scores can help structure discussion but are rarely valid measurements of expected harm. Ordinal labels have no guaranteed equal intervals; multiplying them creates numbers without a defensible ratio scale. A rare fatal incident and a frequent minor delay can receive the same product despite different moral constraints, tail severity and decision urgency. Cox (2008) demonstrates mathematical deficiencies of popular risk matrices, including weak discrimination among risk pairs and ranking reversals. Changing a colour or moving a point in a matrix is not evidence that treatment reduced risk.

For operational use, likelihood and consequence scales should be anchored to explicit time periods, money ranges, service interruptions and nonfinancial harms. Catastrophic safety or legal exposure should be flagged regardless of a multiplication product. Where defensible frequencies exist, managers can use numerical loss distributions and scenario-weighted analyses; where they do not, they should communicate plausible bounds and knowledge limitations. Heat maps become useful as *screening and conversation devices* when supplemented by causal mapping, credible scenarios, tolerances and named action owners. Their misuse begins when an attractive visual substitutes for explicit judgment or assurance.

32.8.3 Expected loss, scenario analysis, sensitivity, and stress tests

For mutually exclusive, exhaustive and sufficiently well-defined scenarios s, expected loss can be written $E(L) = \Sigma\ p_s\ L_s$, where p_s is a justified scenario probability and L_s is the economic loss conditional on that scenario. The model requires non-overlapping outcomes, comparable valuation assumptions and probabilities summing to one. Under high uncertainty, p_s may be unavailable or too unstable for a single-number recommendation. Decision-makers can then use interval probabilities, break-even thresholds, robust comparisons across scenarios and explicit non-negotiable constraints. Loss estimates should separate incremental expenditure, foregone contribution, recoverable stock, insurance recoveries, time-varying obligations and nonmonetizable harms to avoid double counting.

Sensitivity analysis varies one assumption while preserving others; scenario analysis varies a coherent set of related conditions; stress testing asks whether an enterprise can withstand a severe but plausible configuration of losses, cash demands and operational interruptions. These methods answer distinct questions. A stress test designed around an adverse combination is not a forecast that the combination will occur. A reverse stress test asks what combination would breach a survival boundary, such as running out of cash or failing a critical service beyond the maximum tolerable period. It can expose a hidden dependence on a seemingly minor asset or staff member. IEC 31010:2019 presents a selection framework for assessment techniques, not a guarantee that the chosen model's assumptions are satisfied (IEC, 2019).

Table 32.3

Selection and interpretation of principal risk-analysis instruments

Instrument	Best-suited question	Evidence requirement	Principal caution
Dependency map	Where can one failure propagate?	Workflow, supplier and systems evidence	Unobserved links may be omitted
Risk register	What is known, owned and being controlled?	Explicit events, owners, controls and dates	Enumeration is not prioritization
Heat map	Which exposures warrant structured discussion?	Anchored categories and review judgement	Ordinal numbers do not produce cardinal risk
Expected-loss model	Is a repeated intervention economically worthwhile?	Credible event probabilities and loss model	Tail harm and ethical constraints may dominate
Scenario and stress test	What fails under a coherent shock?	Internally consistent time, capacity and cash paths	Severe scenario is not a probability forecast
Business impact analysis	Which activities must recover, by when?	Process dependencies and time-dependent impacts	RTO is a requirement, not an achieved capability
Tabletop and live test	Will a plan work with real roles and tools?	Exercise record, observed time and exceptions	Rehearsal cannot perfectly reproduce a crisis

Note. Original comparison based on ISO (2018), IEC (2019), ISO (2021), and Cox (2008).

32.8.4 Evidence quality and disciplined model use

Every quantitative analysis should declare whether its numbers are measured, estimated from an identifiable population, elicited from specialists, or merely assumed for instruction. This classification prevents the dangerous conversion of a convenient parameter into an asserted empirical fact. Correlation requires particular attention. A transport closure and supplier delay may arise from the same flood; multiplying independently estimated probabilities would understate their joint occurrence if independence is not justified. Equally, costs and lost sales may overlap because a firm cannot sell goods it never received. The analyst should map event sequences, use conditional probabilities where supported, and report sensitivity to dependency assumptions rather than hide them within a single average.

When risk appetite is ambiguous, a manager should not invent a technical cut-off to force apparent agreement. Competing stakeholders may legitimately value the same consequence differently, and some rights cannot be monetized without controversy. A documented decision can still be rigorous if it describes alternative courses, available evidence, worst credible impacts, uncertainty, contested values, accountable authorization and follow-up observation. Formal quantitative models are most useful when they discipline these judgments, not when they pretend to eliminate them (Aven, 2016; Mikes, 2009).

32.8.5 The value and limits of additional information

Risk analysis should guide not only what managers decide, but what evidence they should purchase before deciding. A decision whose preferred option would remain unchanged across all plausible probabilities has little immediate value from further probabilistic estimation. By contrast, where a small change in an uncertain parameter reverses the recommendation, improved observation, a pilot exercise or independent supplier validation may be valuable. A simplified expected-value-of-information calculation compares the expected outcome under present information with that achievable after receiving information, accounting for the cost, timeliness and reliability of the proposed evidence. Perfect information is an idealized analytical bound, not a service available for purchase.

For critical enterprise functions, information value may lie in discovering infeasibility rather than refining an event probability. A live test establishing that two nominal backup providers share a telecommunications network can be more consequential than a more precise estimate of average downtime. Likewise, a daily cash forecast can reveal a borrowing need that an annual expected-loss model obscures. Decisions should also be assessed for reversibility: an expensive irreversible facility investment demands stronger evidence than a modest trial that preserves the option to stop. This reasoning helps explain why robust and staged choices are often appropriate where reliable distributions cannot be estimated (Aven, 2016; Bromiley et al., 2015).

32.8.6 Dependence, compound scenarios, and communicating uncertainty

The probability of two disruptions occurring together is not generally the product of their individual probabilities. That multiplication assumes independence, which can fail when a single flood, power disruption or provider failure affects several systems. A simple illustration uses illustrative conditional probabilities, not estimates of real events. If the probability of a route closure over a defined period is assumed to be 10%, and the probability of a supplier delay *given that closure* is 70%, the modelled joint probability is $0.10 \times 0.70 = 7\%$. Multiplying 10% by an assumed unconditional supplier-delay rate of 20% would instead produce 2%, understating the illustrated joint risk because the dependency was ignored. The 7% number is valid only within the hypothetical assumptions and specified period.

Uncertainty reporting should accompany numerical estimates with the event definition, exposure population, evidence source, period, known omissions, key dependencies and sensitivity to disputed premises. Where risks have severe nonfinancial consequences, loss probability and severity should be displayed separately from the rights-based decision boundary. A model's apparent precision can otherwise conceal incomplete knowledge, inadequate categories or ethically unacceptable aggregation. The most persuasive risk report is one that allows a competent reader to change an assumption, reproduce the calculation and understand whether the managerial choice would change (Cox, 2008; Aven, 2016).

32.9 BUSINESS CONTINUITY AND CRISIS RESPONSE

32.9.1 Continuity management and the business impact analysis

Business continuity management seeks to maintain or resume prioritized activities at predefined, acceptable levels after disruptive incidents. The governing process is not identical to risk reduction: a hazardous event can occur despite strong prevention, so the enterprise must still determine what functions must continue, how quickly, using what resources and at whose authority. ISO 22301:2019 specifies requirements for a business continuity management system and is amended by ISO 22301:2019/Amd 1:2024 regarding climate action considerations; ISO/TS 22317:2021 guides the design of a business impact analysis (BIA) process (ISO, 2019, 2021). These are distinct instruments. Unlike the noncertifiable ISO 31000, ISO 22301 is a requirements standard under which organizations may pursue

third-party certification; certification does not establish that every future crisis will be handled successfully.

The BIA starts with the products and services whose interruption would cause the greatest time-dependent harm. For each, it identifies the associated activities, minimum acceptable delivery level, direct and indirect dependencies, escalating consequences, legal and contractual timing, and recovery needs. The maximum tolerable period of disruption (MTPD) is the point after which the impact becomes unacceptable under specified criteria. A recovery time objective (RTO) is the planned time within which a particular activity or resource should be restored; it should normally be shorter than the relevant tolerable disruption period and should account for the time required to verify safe operations. A recovery point objective (RPO), applicable to data, indicates the maximum tolerable amount of data loss expressed as a time interval. RTO measures target restoration duration; RPO measures the data-restoration point. They should not be confused with observed restoration performance or copied uncritically from a supplier contract.

A reliable BIA does not simply assign all activities an RTO of one hour. The resulting plan would be expensive, operationally impossible and internally contradictory. Instead, it compares the consequences of postponing nonessential tasks with the resources needed to protect safety, legally necessary records, customer commitments and cash. The analysis may reveal that a manually recorded order can be accepted quickly while accounting reconciliation can follow with a controlled lag; or that backup inventory is useless if dispatch cannot access a road. Minimum staffing, independent power, accessible customer contacts, approved workarounds and contractual permissions are part of recovery design.

32.9.2 From recovery objectives to executable procedures

A continuity procedure should identify the activation threshold, authority to declare an incident, task sequence, responsible and alternate persons, required contacts and credentials, safe-work limits, evidence retention, customer messages, supplier steps, financial controls, restoration acceptance tests and a formal return-to-normal decision. A plan stored only in the unavailable cloud application defeats itself. Printed, securely stored or separately accessible critical contact and instruction sets can be appropriate, provided privacy and information-security obligations are observed. Continuity is not a single document but a maintained capability supported by exercises, training, change control, supplier agreements and financial provision.

Crisis management is conceptually distinct from business continuity. A crisis may introduce profound uncertainty, urgency, competing stakeholders and reputational or institutional consequences beyond recovering a process. Pearson and Clair (1998) situate organizational crises within psychological, sociopolitical and technological structures; Weick (1988) explains why sensemaking can deteriorate when actions meant to clarify the situation affect it. ISO 22361:2022 provides guidance on crisis leadership, decisions, communication, training and review (ISO, 2022). A well-configured crisis team therefore needs authority to obtain conflicting information, compare options, protect people, document decisions and communicate provisional knowledge. The executive decision to cease an unsafe dispatch should not require statistical proof of an expected loss.

32.9.3 Crisis roles, communication, and exercises

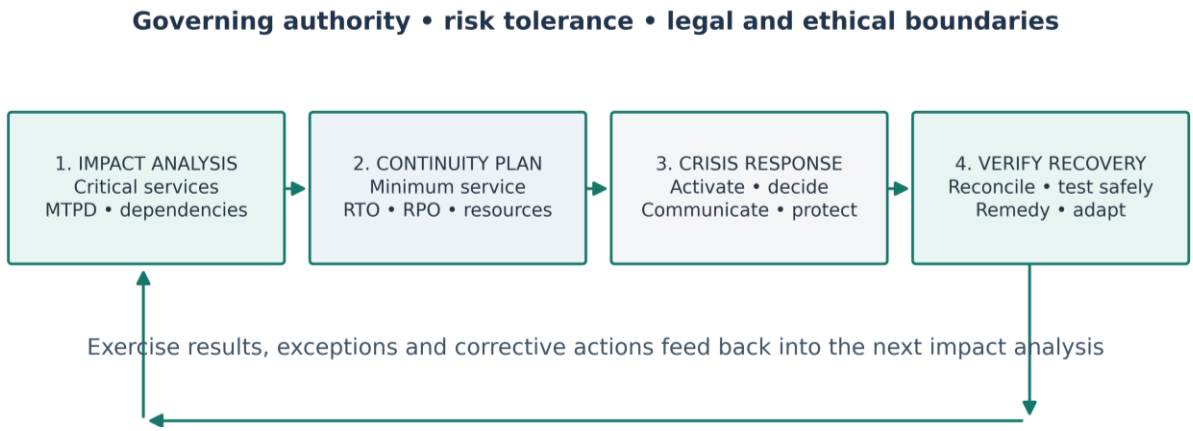
The incident commander or crisis chair directs the response within delegated authority and keeps a single decision record; operations coordinates safe service; finance monitors cash and payments; ICT preserves digital evidence and restores systems; HR safeguards personnel; communications provides accurate updates; and legal or compliance specialists advise when notification, regulatory reporting or contractual deadlines may apply. In a microenterprise, one person may occupy several roles, making a designated alternate and clear escalation to external authorities especially important. The public-facing

message should state what has been established, the immediate customer impact, the next update time and the available alternative route for critical needs. Unsupported promises of imminent recovery are typically worse than honest uncertainty (Boin et al., 2005).

Exercises range from a contact-list check and facilitated tabletop discussion to technical backup restoration, supplier failover and integrated live simulations. Each tests a specified outcome. A tabletop may reveal ambiguous authority but cannot establish the time required to restore a corrupt database. A live recovery test can establish observed time under the tested conditions but does not guarantee performance during an earthquake or region-wide telecoms failure. Exercise evidence should include start and end timestamps, actions, deviations, safety and privacy observations, responsible corrective owners and retest dates. Figure 32.2 locates continuity controls within the wider risk-resilience cycle.

Figure 32.2

Continuity and crisis governance, from business impact to tested recovery.



Note. Original educational process model informed by ISO (2019, 2021, 2022); it does not reproduce proprietary standard text.

32.9.4 Crisis phases, decision cadence, and external coordination

A serious event rarely unfolds according to a fixed response script. During detection, the organization needs verified signals and clear authority to activate a protective procedure. During stabilization, leaders must stop preventable harm and preserve essential information. During constrained operation, they must allocate scarce capacity, communicate realistic commitments and document exceptions. Restoration then requires technical and financial reconciliation, followed by controlled normalization and a post-event review. These phases may overlap, especially when new information changes the understanding of the initial event. Treating them as a rigid chronological staircase can slow response when leadership needs to revisit an earlier decision (Pearson & Clair, 1998; Boin et al., 2005).

A crisis team should operate at an explicit decision cadence. In the first hours of a significant payment and transport incident, an appropriately small group may need frequent short reviews to reconcile new facts, authorize priority spending and issue customer updates; later, the cadence can be reduced as the situation stabilizes. Each decision record should identify known facts, material unknowns, alternatives considered, reasons for the chosen action, who was consulted, and the time for reconsideration. This is particularly valuable where verbal instructions or separate messaging groups otherwise generate contradictory decisions. A single common operating picture improves coordination, but it should include sources and confidence levels rather than suppress dissent for the sake of a uniform narrative.

External coordination may be indispensable. Road authorities, payment providers, emergency services, health regulators, insurers, lenders, sector associations and local government may each hold information or powers unavailable to the enterprise. A continuity plan should specify when contact is required and distinguish requests for assistance from formal legal notifications. Where a disruption affects essential

community services, enterprise-level prioritization must be compatible with public safety and transparent allocation. ISO 22361 offers guidance for strategic crisis capabilities, but it does not replace official emergency commands or country-specific regulatory duties (ISO, 2022; UNDRR, 2015).

32.10 ENTERPRISE RESILIENCE CAPABILITIES

32.10.1 Redundancy, flexibility, adaptability, and option value

Resilience capacity is often described as a stock of buffers or a capacity to change. These are competing but potentially complementary mechanisms. Redundancy preserves spare inventory, funds, vehicles, labour or data copies for an interruption; flexibility permits the organization to redirect existing resources when conditions change; adaptability permits it to revise routines, products and arrangements after learning that assumptions no longer hold. Sheffi and Rice (2005) stress the distinction between redundancy and flexibility in supply networks. Duchek's (2020) anticipation-coping-adaptation account provides an organizational vocabulary for these capabilities. Neither approach means that all slack is desirable. Excess cash buffers can restrict investment; excessive stock can expire; idle capacity can undermine affordability; and multiple providers can require complex reconciliation and more attack surfaces.

Real-options reasoning reframes selected resilience expenditures as the purchase of a contingent choice. An enterprise might pay a modest amount to maintain a prequalified alternate carrier without using it during normal operations. This option has value when the primary route fails and the alternative can actually be exercised. A defensible comparison accounts for the fee, exercise cost, probability or range of disruptions, avoided incremental losses, operational constraints, correlated provider exposure, and irreducible nonfinancial harms. Expected monetary value is only part of the decision when legal duties or the possibility of catastrophic harm are involved. The Rwanda case in Section 32.13 calculates a break-even disruption probability for such an option rather than pretending that the probability is known.

32.10.2 Organizational learning and the problem of resilience metrics

A firm can invest heavily in visible emergency assets while neglecting practice and institutional memory. In contrast, a modest but repeatedly tested plan may work reliably because staff recognize when to escalate, where records are available and who can authorize substitutions. Learning requires accurate near-miss reporting, analysis of both successful and failed workarounds, documented changes, and observation of whether a modified practice actually improves performance. Repenning and Sterman (2001) caution that organizational systems can undermine improvement when urgent production demands displace preventive investment. Thus a resilience programme should fund testing, not merely preparedness documents, and protect time for correction after exercises.

Performance indicators should distinguish preparedness, response, outcome and learning. Leading indicators include the share of critical dependencies with confirmed alternatives, the age of BIA reviews, control-test completion and restoration evidence. During an event, meaningful indicators include time to detection, activation time, proportion of priority orders fulfilled safely, peak liquidity gap and unmet stakeholder needs. After an event, recovery time, total losses, service restoration quality and verified action closure are useful, but each must be interpreted against severity and context. A shorter recovery time is not automatically superior if achieved through unreported unsafe work or inaccurate customer charges. Indicators should carry definitions, denominators, measurement periods and evidence owners, just as financial metrics do elsewhere in the book.

32.10.3 Capability-building in different enterprise forms

Large multinational groups may require dedicated risk teams, independent assurance, multi-location failover, formal exercise programmes and group-wide risk aggregation. A cooperative may instead need elected-member oversight, transparent authorization to use common funds, a safe paper register, multiple purchasing relationships and a democratically legitimate emergency decision. A sole proprietor can strengthen resilience through duplicate contacts, a verified backup of sales records, an alternate supply arrangement and a modest cash buffer. These arrangements are not categorically inferior because they are less formal. Their adequacy depends on the harm potentially caused by interruption, the enterprise's actual resources and the complexity of its network (Herbane, 2010). Risk controls that cannot be maintained or tested provide uncertain protection regardless of how impressive they look in policy documents.

32.10.4 Measuring genuine capability rather than preparedness expenditure

The central measurement challenge is that capabilities are partly latent until tested. Spending on backup systems, insurance and consultant assessments is an input; the existence of a signed plan is an intermediate output; safely restored essential service is an outcome. The three should never be reported as interchangeable evidence of resilience. A credible management scorecard therefore distinguishes the proportion of critical functions covered by a current BIA, the proportion of alternatives actually exercised, observed restoration durations, the share of unresolved high-consequence defects, exposure to common providers, and stakeholder complaints that remain without remedy. A target should state its numerator, denominator, observation window and source, and a failed exercise should be treated as information rather than automatically as managerial disgrace.

The cost of improvement must be evaluated with complementarity in mind. Buying a backup communication service has little value if staff do not know how to activate it, customer contact details are inaccessible or supplier terms prohibit the planned workaround. Conversely, training without protected time, minimum equipment and delegated authority is unlikely to sustain difficult restoration. The enterprise should fund combinations of controls whose prerequisites make them usable, then test the integrated configuration rather than celebrating purchases separately. ISO 22316:2017 supplies principles and attributes for organizational resilience, while the capability-based studies by Duchek (2020) and Lengnick-Hall et al. (2011) help explain why resources, judgement and learning must be connected. These are theoretical and professional contributions, not a claim that certification or a high dashboard score causally guarantees survival.

32.11 INTERCONNECTED CRISES AND SYSTEMIC EFFECTS

A systemic disturbance travels through common infrastructure, networks, markets or institutional dependencies so that losses across organizations become correlated. Climate-related flood damage can close transport routes, interrupt power, affect worker access, delay supplies, alter food prices and restrict cash collections simultaneously. Currency instability can increase import costs while reducing customers' purchasing power. Telecommunications interruption may prevent both payment confirmation and coordination with the alternative carrier that a continuity plan assumed would remain reachable. These connections mean that summing separately assessed departmental risks can materially misrepresent enterprise-level exposure. An aggregate strategy should examine common causes, feedback loops, correlated resource shortages and the possibility that response measures worsen other harms.

The May 2023 floods and landslides in Rwanda demonstrate why physical hazards have economic and social dimensions. On 6 May 2023 the Government of Rwanda reported 131 deaths and serious damage to infrastructure across affected provinces; it also announced intended mobilization of more than RWF 110 billion for infrastructure reconstruction (Government of Rwanda, 2023). These are dated government-

reported figures and plans, not a definitive final loss account or a measure of the losses of the hypothetical firm examined below. Their relevance is the documented possibility that transport and public infrastructure disruptions affect lives and enterprise operations together. Risk governance must not trivialize such events as a delivery delay or treat communities solely as logistical obstacles.

The National Institute of Statistics of Rwanda (NISR) reported approximately 278,060 business enterprises in its 2024 Integrated Business Enterprise Survey, with informality accounting for at least 87% of the business landscape (NISR, 2026). Its survey definition of formal enterprise depends on registration and regular business accounts; it should not be equated mechanically with all legally or economically active organizations. This context changes how resilience advice can be implemented. A method dependent on specialist risk software, actuarial histories and complex committees is unlikely to be proportionate for most microenterprises. Yet small scale does not eliminate systemic dependence: a trader reliant on one payment provider and one transport corridor may be highly exposed even when its internal operation is simple. The appropriate response combines feasible enterprise-level safeguards with attention to public infrastructure, market competition, accessible finance and institutional capacity.

The United Nations Sendai Framework for Disaster Risk Reduction 2015–2030 emphasizes understanding disaster risk, strengthening governance, investing in resilience and improving preparedness and recovery (UNDRR, 2015). It is a policy framework with broad relevance, not proof that a particular private investment will succeed or an automatic source of national corporate legal duties. For business, it supports recognition that resilience cannot be purchased solely within a firm's walls: public roads, reliable power, transparent information, social protection, functioning health services and credible emergency institutions condition organizational recovery. Chapter 31 examines sustainability and environmental effects in depth; the present section emphasizes crisis propagation and the business consequences of systemic fragility.

A critical systems view must also ask who receives priority. When a shortage occurs, a powerful buyer may secure the last available stock, leaving schools, small retailers or lower-income households without essential goods. Crisis procurement may invite price gouging, favouritism or exclusion. An ethical continuity policy can specify protected critical customers, transparent rationing criteria, minimum safety and legal standards, a grievance route and a documented procedure for allocating scarce capacity. Such provisions do not eliminate conflict. They make the choices visible to challenge and prevent a model calibrated only to profit from being mistaken for a comprehensive social assessment.

32.11.1 Cascades, cross-border exposure, and public infrastructure

Compound events are analytically different from coincidental single risks. A flood may simultaneously reduce transport capacity, increase delivery lead times, constrain attendance, damage inventory and delay customer payments. One failure then changes the severity of another: a delayed shipment increases working capital exposure, insufficient cash constrains alternative sourcing, and reduced supply intensifies customer competition for scarce stock. This feedback loop cannot be represented reliably by simply adding stand-alone heat-map scores. Systems analysis instead identifies initiating conditions, propagating channels, thresholds, scarce resources and the interventions that can interrupt escalation. The resulting dependency map should be updated after structural changes and should distinguish genuine common causes from correlations observed in a short period.

Rwandan enterprises can be affected by disruptions outside their immediate geographic boundaries through imported supplies, regional routes, payment correspondents and foreign-currency settlement. Yet a firm-level analysis should not equate membership in a regional trading arrangement with guaranteed access to a particular alternative road, product or payment service. Border documentation, restrictions, standards, carrier networks and actual operating capacity still matter. A practical regional scenario therefore evaluates whether the alternate pathway is legally accessible, whether a carrier can provide

capacity under correlated demand, what full delivered cost is incurred and whether customer commitments can be revised lawfully. These details connect the present chapter with the operational logistics and regional-trade analysis of Chapters 19 and 30 without duplicating their full technical scope.

32.11.2 Distributional exposure and the limits of enterprise self-protection

Infrastructure vulnerability introduces a public-good dimension to resilience. Private controls can lessen some consequences, but roads, flood protection, dependable energy, public health and credible emergency information are jointly supplied and cannot always be recreated by an individual microenterprise. Policy intervention and institutional coordination may therefore be efficient even where private emergency procurement appears expensive. Conversely, public infrastructure investment should not be justified by vague assertions of business benefits alone; it requires evidence on exposure, alternative projects, distributional impact and financial capacity. The Sendai Framework provides relevant international priorities, but specific policy choices require domestic analysis (UNDRR, 2015).

Distributional questions become especially consequential when firms are connected through unequal bargaining power. A large buyer may protect its own operations by delaying payment to a smaller supplier, whose subsequent failure disrupts many local businesses. A strong importer may reserve scarce transport capacity while less powerful traders cannot access basic goods. These choices may enhance the resilience of one balance sheet while weakening the wider ecosystem. Accordingly, enterprise risk registers should record material risks *to others* as well as risks *from others*, especially where contractual leverage, working conditions and community dependence create foreseeable harm. Ethical governance requires an accountable reason for prioritization and accessible procedures for correction, not an unsupported assertion that commercial continuity always serves the public interest.

32.12 RECOVERY AND ADAPTIVE LEARNING

Recovery is not complete when an application restarts or an order book resumes. It requires verification that data are reliable, customers have been correctly charged, products remain safe, workers have reasonable conditions, contractual records are reconciled and the organization can sustain the restored activity. A premature declaration of normality can generate second-order incidents through untested workarounds, accumulated backlogs, rushed maintenance and missing evidence. Crisis leaders should therefore distinguish emergency stabilization, controlled restoration, reconciliation, transition to ordinary governance, and adaptive redesign. Pearson and Clair's (1998) multidisciplinary perspective is valuable because perceived legitimacy, human consequences and technical restoration are not reducible to a single recovery indicator.

A post-event review should reconstruct the timeline from independently traceable records and participants' accounts; distinguish observations from hindsight; assess whether signals were available before the incident; investigate delays and contradictory instructions; evaluate stakeholder harms and compensatory duties; and rank changes by feasibility, expected consequence and rights. "Root cause" may be a useful practical term, but complex events often have several jointly necessary conditions rather than one removable cause. An unqualified blame narrative may silence the very information required for improvement. A defensible review assigns corrective action owners, realistic due dates, independent verification and a scheduled retest. Findings should be translated into procurement conditions, contract clauses, staff development, architecture changes, cash policy and revised BIA assumptions rather than confined to the risk office.

Rebuilding provides an occasion to evaluate whether the previous system deserves restoration. A firm whose primary supplier repeatedly failed may redesign its product mix; one whose customer communication worked through simple channels may preserve a low-technology fallback; one whose

digital controls obstructed timely humanitarian response may revise delegated authority without abandoning privacy and auditability. Learning therefore includes selective abandonment of outdated routines. Duchek's (2020) distinction between coping and adaptation illuminates the shift from returning to pre-event operation to improving the capacity to meet legitimate objectives under changed conditions. This shift must be judged empirically through subsequent tests and outcomes rather than claimed because the organization rewrote its policy.

Table 32.4

Post-incident accountability and learning protocol

Review element	Required evidence	Test of adequate closure
Event sequence	Timestamped system, payment, dispatch and decision records	Conflicting accounts resolved or uncertainty disclosed
Consequence map	Customers, staff, cash, safety, privacy and supplier impacts	Material omitted consequences investigated
Control diagnosis	Intended safeguard, actual operation and observed failure mode	Evidence distinguishes design from operating failure
Remedy and redress	Correction, customer notification, contractual and regulatory steps	Affected parties have documented routes for remedy
Adaptation decision	Alternatives, costs, feasibility and accountable approval	Change is implemented and independently checked
Retest and learning	Tabletop/live test, observations and action closure	Critical recovery objectives met in specified test conditions

Note. Author-developed protocol informed by Duchek (2020), Pearson and Clair (1998), and ISO (2022). A review is not independent assurance unless appropriate independence and scope are established.

32.12.1 Recovery assurance, counterfactual judgement, and institutional memory

Post-event improvement is easily distorted by hindsight. Once a failure is known, previously ambiguous evidence can seem obvious and the chosen action can appear irrational even when the ex ante alternatives were genuinely uncertain. A disciplined review reconstructs what was knowable at successive decision points and distinguishes a deficient process from an unfavourable outcome. This prevents rewarding reckless decisions that succeeded by chance or punishing defensible decisions merely because an extreme event occurred. The counterfactual question should be framed carefully: *Given the evidence then reasonably available, which feasible alternative action might have changed the outcome, through what mechanism, and with what cost or rights implications?* Where records are incomplete, the review should state its uncertainty rather than invent a tidy narrative.

Assurance after recovery requires more than a signed completion form. Independent or appropriately separated reviewers should test whether reconciliation was accurate, customers received corrections, restored systems have secure controls, alternative suppliers remain available and exercises verify promised recovery times. Closure is incomplete if a critical corrective action was approved but not implemented, or if a replacement procedure creates a previously unrecognized dependency. A well-managed event review therefore produces traceable decisions, accountable owners, due dates, test evidence, remaining risk and the authority that accepted any unresolved exposure. Institutional memory can be supported through controlled versions of plans, training of alternates and periodic retesting, rather than relying exclusively on staff who happened to participate in the last crisis (Duchek, 2020; ISO, 2022).

32.12.2 Recovery as an ethically accountable redesign choice

The return to ordinary commercial activity is not always the morally or strategically best endpoint. An enterprise may discover that its previous supply arrangement was unsafe, its emergency communications excluded customers with limited connectivity, or its stock allocation left highly dependent customers without necessary goods. Recreating the pre-event arrangement would restore a known vulnerability. A more defensible redesign evaluates economic viability, safe service, operational evidence and the legitimate claims of affected parties. Where a change would impose disproportionate costs on workers, consumers or weaker partners, it should be revisited even if its financial case appears favourable.

Resilience research also needs to distinguish restoration from transformation. A firm that permanently narrows its customer base may restore profitability quickly while leaving vulnerable clients without access; another may temporarily accept higher operating cost to maintain essential service and retain trust. Neither decision can be evaluated fully through a single speed-to-recovery metric. Outcomes should therefore include quality, accessibility, remedy, cash survival and the future adaptability of the service system. This broader account prepares the transition to Chapter 33's detailed examination of business ethics without claiming that a conceptual model resolves every competing moral or stakeholder demand.

32.13 RWANDA-CENTRED APPLICATION: CONTINUITY DESIGN FOR A KIGALI DISTRIBUTOR

32.13.1 Context, decision problem, and evidence boundaries

The fictional enterprise in this case, Kigali Essential Distribution Ltd. (KED), purchases packaged household essentials from domestic and regional suppliers and supplies institutions and small retailers in Kigali. It is a constructed educational entity; its name, revenues, contracts, disruption probabilities, losses and resources are assumed solely to permit independently reproducible analysis. The business context is informed by Rwanda's documented predominance of micro and informal enterprises, its rapid expansion in financial services and its exposure to physical transport disruptions, but no public dataset is claimed to describe KED's performance (NISR, 2026; NBR, 2025; Government of Rwanda, 2023).

KED faces three possible linked shocks: a payment-provider interruption prevents real-time receipt confirmation; a damaged route reduces dispatch capacity; and its principal supplier delays replenishment. The owner must decide whether to pay an annual retainer for alternate carrier and supply access, establish manual order and payment verification, and arrange a contingent liquidity facility. The problem is not to calculate a colour-coded score, but to protect a minimally acceptable service, honour customer and staff obligations, and choose a feasible treatment under substantial uncertainty. KED can reasonably prepare for a disturbance without claiming that a specific future flood or national payment-system breakdown will occur.

32.13.2 Critical service and dependency reconstruction

The first step is a process walk-through, not a technology purchase. Customer service accepts orders; sales confirms terms; finance verifies payment or approved credit; inventory staff reserve stock; dispatch checks route and carrier; procurement replenishes; ICT maintains records; and management resolves exceptions and communicates with affected customers. The dependencies are two-way. An unverified payment blocks authorized release; a delayed supplier reduces the value of a functioning payment interface; and an unapproved manual record can produce duplicate collections even after digital service returns. Any alternate arrangement must therefore have separate procedures for authorization, transaction evidence, reconciliation, customer notification and safe dispatch.

Table 32.5

Illustrative business impact assessment for KED

Essential activity and minimum acceptable service	Critical dependencies	Maximum tolerable disruption	Target recovery time; data RPO	Accountable owner
Order reception and customer updates: accept priority orders and communicate revised commitments	Staff, protected contacts, order log, alternate communications	24 hours	RTO 4 hours; RPO 1 hour for orders	Commercial lead
Payment verification: confirm receipts or record explicitly authorized deferred settlement	Provider, bank, reliable records, approval rights	16 hours	RTO 8 hours; RPO 1 hour for receipts	Finance lead
Safe priority dispatch: deliver at least 40% of priority volume	Available stock, route, carrier, safe workers	48 hours	RTO 24 hours; RPO 4 hours for stock	Operations lead
Replenishment: secure a feasible supply commitment	Approved alternative, financing, specification, transport	10 days	RTO 5 days; RPO not applicable	Procurement lead
Payroll: meet lawful wage commitments or activate an authorized remedy	Cash, bank access, records, legal duties	3 days	RTO 2 days; RPO 24 hours for working data	Finance and HR leads
Customer record integrity: reconcile manual and restored transactions	Protected backup, controlled paper log, trained staff	24 hours before material integrity risk	RTO 12 hours; RPO 1 hour for critical data	Data and finance leads

Note. All service levels and time thresholds are hypothetical planning requirements, not measured recovery performance. Each MTPD needs owner validation against contractual duties, safety, financing and affected customers. An RTO shorter than MTPD is a target requiring a demonstrated recovery method.

The BIA reveals that a single route cannot satisfy the dispatch RTO if the alternative carrier uses the same blocked road. For that reason, the contingency contract should explicitly cover alternative routings and vehicle availability, and the chosen transport partner should complete a practical test. Similarly, an offline order book does not automatically solve the payment problem: finance must define which customers may receive approved deferred settlement, who can authorize the limit, how duplicate transactions are detected, and when accounting records are reconciled. The company should not claim to meet a one-hour RPO unless a restoration test demonstrates that its backup process actually preserves recoverable data to that point.

32.13.2.1 Assurance of proposed recovery arrangements

A BIA is a specification of need, not proof of capability. The listed targets should therefore be approved by accountable owners after comparing interruption consequences, statutory duties, actual resources and the results of a practical restoration exercise. For example, a four-hour order-reception objective depends on staff being able to access customer contacts, identify authorized account terms, establish a safe alternative channel and protect personal data. A nominal one-hour data RPO depends on the frequency and integrity of recoverable copies. If an offline register can continue receiving orders but cannot reconcile them accurately later, the organization has not met a credible continuity objective. This distinction

prevents the table from becoming a collection of administratively convenient but technically untested targets.

The minimum dispatch service of 40% is also an assumption requiring scrutiny. A 40% overall delivery rate could conceal complete failure to deliver the most critical items if managers select only the easiest routes and largest customers. The exercise should therefore assess priority fulfilment by agreed customer class and product criticality while recording worker safety and product integrity. If the proposed carrier cannot provide a route that remains available during a flood, management should redesign the alternative rather than certify the target as achieved. These qualifications make the RTO and service-floor figures explicit teaching premises rather than inferred Rwandan industry benchmarks (ISO, 2021; Christopher & Peck, 2004).

32.13.3 Reproducible five-day interruption-loss model

Assume KED ordinarily sells RWF 4,000,000 per trading day; its avoidable variable costs are 70% of sales, giving an incremental contribution margin of 30%. Five equivalent days of completely lost eligible sales would therefore put RWF 20,000,000 of revenue and RWF 6,000,000 of contribution at risk. This amount is not the same as lost net profit: unavoidable fixed costs continue in both states and should not be deducted a second time. For illustration, assume a severe five-day compound event also causes RWF 1,800,000 of otherwise unrecoverable inventory impairment, RWF 1,200,000 of extraordinary operational expenditure and RWF 700,000 of substantiated customer claims. Total modelled event cost without the proposed alternative is RWF 9,700,000, assuming these components are separate and not already incorporated into variable costs or customer losses.

Table 32.6

Scenario loss bridge, stated in RWF

Loss component	Formula or assumption	Without contingency
Lost sales revenue, not itself a net economic loss	4,000,000 × 5	20,000,000
Lost contribution	20,000,000 × (1 − 0.70)	6,000,000
Unrecoverable damaged or obsolete stock	Constructed incremental assumption	1,800,000
Extraordinary incident expenditure	Constructed incremental assumption	1,200,000
Contractually substantiated claims	Constructed incremental assumption	700,000
Total modelled event loss	**6,000,000 + 1,800,000 + 1,200,000 + 700,000**	**9,700,000**

Note. The stock and claims amounts are assumed distinct from the contribution calculation; otherwise subtracting them again would overstate loss. Revenue at risk is shown to clarify scale and is not added to total event loss. The costs are hypothetical and exclude nonmonetary harm.

The alternative carrier and supplier arrangement is assumed to restore 60% of normal sales on days 2–5, with no recovery on day 1. This protects the equivalent of 2.4 full trading days, or RWF 9,600,000 in sales, yielding RWF 2,880,000 of contribution. Assume the arrangement further prevents RWF 900,000 of stock impairment and RWF 200,000 of legitimate claims. Its gross measurable avoided loss is therefore RWF 3,980,000. If exercising the arrangement requires RWF 1,100,000 in incremental fees, the net benefit conditional on the illustrated event is RWF 2,880,000. Remaining event loss is RWF 6,820,000, computed as RWF 9,700,000 − RWF 3,980,000 + RWF 1,100,000. The retainer, which is paid regardless of whether the event occurs, must be kept separate from these conditional amounts.

Table 32.7

Testable resilience-investment decision under assumed event probabilities

Decision quantity	Formula	Result
Avoided contribution	4,000,000 × 0.30 × 4 × 0.60	RWF 2,880,000
Other avoided losses	900,000 + 200,000	RWF 1,100,000
Gross event-contingent benefit	2,880,000 + 1,100,000	RWF 3,980,000
Event-contingent implementation cost	Stated assumption	RWF 1,100,000
Net benefit if specified event occurs	**3,980,000 – 1,100,000**	**RWF 2,880,000**
Annual access retainer	Stated assumption	RWF 650,000
Break-even annual probability	650,000 ÷ 2,880,000	22.57%
Net expected annual advantage at 15%	0.15 × 2,880,000 – 650,000	–RWF 218,000
Net expected annual advantage at 30%	0.30 × 2,880,000 – 650,000	RWF 214,000
Net expected annual advantage at 45%	0.45 × 2,880,000 – 650,000	RWF 646,000

Note. Event probabilities are illustrative sensitivity assumptions, not estimates from historical data. The table assumes at most one qualifying event per year, no additional residual retainer obligations and unchanged conditional effects. Discounting and multiple-event paths would be required for a multiyear appraisal.

The annual retainer is economically favourable in the simple expected-value model only when the decision-maker's justified annual probability exceeds approximately 22.57%; no empirical basis is available here for selecting 30% as the true rate. Even below the break-even point, a firm might reasonably prefer the contingency if it protects worker safety, prevents an unmanageable liquidity failure or protects a critical public-facing service. Those reasons need explicit documentation rather than an invented monetary benefit. Conversely, a plan that appears financially attractive may be infeasible if the supplier cannot fulfil its prequalification or the carrier uses the same blocked route. A procurement trial and live dispatch exercise should therefore be conditions precedent to approval.

32.13.4 Liquidity stress and the distinction between expected value and survival

A separate five-day liquidity scenario assumes opening unrestricted cash of RWF 7,000,000, confirmed emergency-period collections of RWF 1,000,000, essential supplier payments of RWF 3,400,000, payroll of RWF 1,200,000, scheduled rent and debt service of RWF 1,500,000, and contingency activation costs of RWF 1,100,000. The simplified closing cash estimate is RWF 800,000: 7,000,000 + 1,000,000 − 3,400,000 − 1,200,000 − 1,500,000 − 1,100,000. If management has previously justified a minimum cash floor of RWF 2,000,000, the closing gap is RWF 1,200,000. This is a *minimum illustrated shortfall relative to the floor*, not a proven maximum borrowing requirement: the daily timing of payments and collections might create a worse intra-period trough. A rolling dated cash ledger is therefore mandatory before executing the arrangement.

The owner might consider an independently available committed line, negotiated supplier deferral, reduced nonessential expenditure or staged activation of the contingency. Each option has different costs and obligations. Supplier deferral should not be an automatic way of financing resilience by imposing distress on a smaller partner. A credit facility is not a confirmed buffer until availability, conditions, currency, cost and permitted use have been checked. A safety and payroll constraint should not be waived to improve the numerical projection. This example shows why positive expected financial value and short-

term feasibility are distinct questions: a contingency may reduce total event loss while bringing forward enough cash expenditure to threaten immediate survival.

32.13.4.1 An illustrative intra-period cash path and financing test

The closing cash calculation is necessary but insufficient, because the order in which collections and payments occur can breach a survival threshold earlier. To demonstrate this, allocate the original five-day totals across the period as follows, all in RWF millions. Start with 7.0. On day 1, collect 0.1 and pay 1.5 of essential suppliers plus 1.1 of activation costs, leaving 4.5. On day 2, collect 0.2 and pay 1.0 to suppliers and 0.6 in wages, leaving 3.1. On day 3, collect 0.1 and pay 0.9 of supplier obligations and 0.9 of rent or debt service, leaving 1.4. On day 4, collect 0.3 and pay 0.6 of wages, leaving 1.1. On day 5, collect the remaining 0.3 and pay the remaining 0.6 in rent or debt service, leaving 0.8. The sequence reconciles exactly with the disclosed total inflows of 1.0 and outflows of 7.2, and it breaches the RWF 2.0 million floor from day 3. The exercise demonstrates a dated cash trajectory; the timing remains hypothetical and has not been observed at any enterprise.

For comparison, under these same assumed operating flows but *without* paying the RWF 1.1 million activation cost, the ending cash would be RWF 1.9 million, still RWF 0.1 million below the floor. Thus the original option is not solely responsible for the liquidity breach; it increases the modelled minimum gap by 1.1 million. This is a distinction with practical consequences. A board that approves the continuity retainer should also approve an executable bridge-liquidity arrangement or a tested alternative spending sequence, not rely upon a favourable expected-value calculation. The funding solution must be separately checked against interest costs, covenants, availability, repayment timing and the treatment of smaller creditors.

32.13.5 Crisis activation, authority, and stakeholder communication

KED's proposed activation rule is operational rather than decorative. After two hours of unverified receipts, finance opens the controlled fallback register and halts unauthorized dispatch. After six hours of material transport interruption, operations escalates to the director and requests an independently verified alternative route. When projected cash falls below RWF 2,000,000 or a safety condition is not met, the director pauses discretionary commitments and authorizes only safe and legally defensible priorities. The control group includes the director, finance, operations, procurement and customer-service leads; alternates are specified for absent role holders. The crisis log records timestamp, observation, decision, authorizer, expected consequence and next review time.

The customer communication protocol should distinguish confirmed orders from orders awaiting payment verification, explain the interruption without attributing unverified causes, offer an estimated update interval instead of an invented delivery guarantee, and provide a clear process for disputed payments. Priority dispatch must follow explicit criteria, such as contractual criticality and immediate harm, while treating small customers fairly. Workers need safe routes, accurate instructions and assured access to concerns and grievance mechanisms. When electronic systems resume, finance and ICT reconcile every manual transaction against provider records before classifying it as settled. Management then verifies stock levels, outstanding customer obligations, retained personal data and incident expenses prior to declaring normal operation.

32.13.6 Continuity testing schedule and management evidence

Table 32.8

Twelve-month continuity exercise and assurance schedule for KED

Timing	Exercise and scope	Measurable acceptance criterion	Evidence and accountable owner

Timing	Exercise and scope	Measurable acceptance criterion	Evidence and accountable owner
Month 1	Validate contacts, delegated authority and offline forms	All critical contacts reachable; alternates acknowledge duties	Signed register; director
Month 2	Payment outage tabletop and duplicate-payment drill	All simulated receipts traceable; no unauthorized release	Reconciliation log; finance
Month 3	Restore backup order and inventory records	Orders restored to within 1 hour; stock records to within 4 hours; completeness checked	Timestamped restoration report; ICT
Month 4	Alternative carrier route and dispatch trial	Safe priority dispatch demonstrably feasible within 24 hours	Carrier confirmation and test manifest; operations
Month 6	Supplier failover and product-quality verification	Substitution meets specification and replenishment objective	Prequalification and test order; procurement
Month 8	Compound payment, route and vendor scenario	Crisis activation, communications and cash pathway completed	Independent observation and action list; director
Month 10	Retest all material corrective actions	High-priority deficiencies corrected and verified	Closure register; independent reviewer
Month 12	Governance review and BIA refresh	Appetite, critical services, owners and RTOs formally reapproved	Decision minutes and version control; governing owner

Note. Timing is a proposed teaching schedule, not a record of completed exercises. The targets are one hour for orders and four hours for stock; an exercise may fail the target and must record failure transparently.

The central professional deliverables are an approved BIA, tested fallback procedures, a controlled risk register, a dated cash stress model, signed third-party commitments, actual test records and an action closure log. The schedule should be adjusted after material system or supplier changes and immediately after significant incidents. Its effectiveness cannot be inferred from completion of eight calendar entries; it depends on whether critical restoration objectives were observed, failures corrected and residual constraints openly accepted by the proper authority.

32.14 INTERNATIONAL COMPARISON AND CONTEXTUAL TRANSFERABILITY

A documented international case illustrates common-cause digital dependency. A.P. Møller–Mærsk reported that its transport and logistics businesses were affected by the NotPetya cyberattack in June 2017. Its contemporaneous investor announcement described systems being taken down, customer disruptions and manual workarounds, while the 2017 annual reporting placed associated losses in the order of USD 250–300 million (A.P. Møller–Mærsk, 2017, 2018). This is company-reported historical evidence, not an independent causal estimate of which resilience investments would have prevented the loss. It nevertheless demonstrates the possibility that software compromise becomes a logistics, customer and financial event rather than remaining an ICT issue. An organization with vessels, ports and global networks has capabilities and dependencies profoundly different from a Kigali distributor; copying the form of its crisis operation would be misguided, while learning to preserve independent communications and manual operating capacity may be transferable.

International standards should be treated similarly. ISO 31000 provides adaptable risk-management principles; COSO connects risk with strategy and performance; ISO 22301 specifies continuity-management-system requirements; ISO/TS 22317 explains BIA methods; ISO 22361 addresses strategic crisis leadership; NIST CSF 2.0 supports cyber-risk coordination; and the IIA's 2026 model clarifies

governance and assurance roles (COSO, 2017; IIA, 2026a, 2026b; ISO, 2018, 2019, 2021, 2022; Pascoe et al., 2024). These instruments are complementary but not interchangeable. None should be represented as an empirical guarantee of organizational survival or as universally binding Rwandan legislation. Their fit depends on enterprise size, sector, mandated standards, network criticality and available capacity.

The comparison is best expressed as a problem of functional equivalence rather than imitation. A global logistics company may operate distributed backup facilities; an SME may maintain an encrypted offline customer list and a verified independent connection. The underlying purpose, continued authorized service with reliable information, is similar, but the design and cost differ. A mature company may use quantitative tail-risk modelling; an owner-managed enterprise may use carefully reasoned severe scenarios and a tested cash buffer. Neither is intrinsically superior without examining its decision context, evidence and potential harms. The transferability test asks whether the mechanism is relevant, whether necessary prerequisites exist, whether the control is maintainable, whether legal and contractual duties permit it, and whether an actual exercise demonstrates its effect.

32.14.1 What international evidence can and cannot establish

The Mærsk experience is informative precisely because its documentary evidence has clear boundaries. The company's annual report records the scale of its reported losses and identifies disrupted functions. It does not provide a randomized comparison between alternative continuity investments or establish which single control would have prevented the incident. Causal attribution of a resilience intervention would require evidence of the pre-existing architecture, feasible alternatives, the sequence of failures, resource requirements and appropriate counterfactual assumptions. It would be unsound to divide reported loss by firm size and apply the quotient to a Rwandan distributor. Such arithmetic would conceal differences in dependency structures, asset intensity, contractual scope and global operating exposure.

The stronger comparative lesson is methodological. International cases should be read for mechanisms that might be portable, such as the need for independently accessible records, credible incident authority, authenticated manual workarounds and tested recovery paths. Before transferring them, the analyst should assess local connectivity, cash buffers, staff capability, legal requirements, feasible supplier contracts and the significance of public infrastructure. Bhamra et al. (2011) and Herbane (2010) help explain why the relevant unit is not the large formal corporation alone. They also caution against equating modest formal documentation with absence of practical adaptive capability. Formality and capability must be measured separately rather than presumed to coincide.

ISO 22316:2017 is particularly useful here because it addresses organizational resilience as a context-sensitive set of principles and attributes rather than a uniform technical configuration. Its guidance complements ISO 22301's specified continuity-management-system requirements, which address a narrower management discipline. Neither replaces the judgement required when a small enterprise must decide whether its first resilience expenditure should buy a second communications pathway, supplier diversification, trained substitutes or emergency liquidity. The appropriate choice depends on the actual critical service and its binding failure mode (ISO, 2017, 2019; Duchek, 2020).

32.15 INTEGRATIVE DISCUSSION: FROM DEPARTMENTAL CONTROL TO RESPONSIBLE ENTERPRISE RESILIENCE

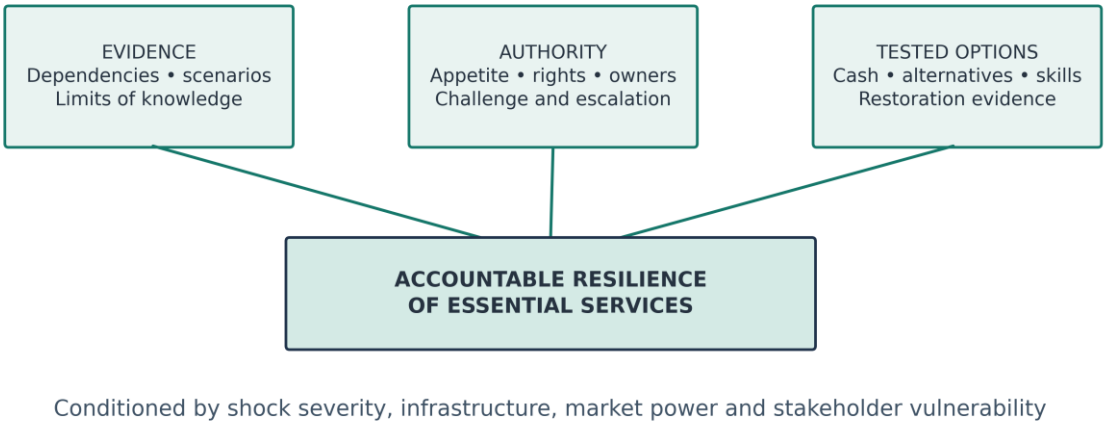
This chapter’s central synthesis is that resilience is a cross-functional property only insofar as critical interfaces have been identified, governed and tested. One department may be individually well managed yet contribute to enterprise failure when its decisions create unrecognized dependence elsewhere. Procurement can secure the cheapest vendor but expose continuity to a single input; finance can minimize idle cash but remove the buffer needed for exceptional purchases; ICT can centralize data efficiently but

create a shared outage; marketing can promise uninterrupted service before operations has demonstrated recovery capacity. Accordingly, ERM must evaluate the interactions among functional objectives rather than accumulate the risks reported separately by each manager.

Figure 32.3 presents a conceptual accountability model in which disciplined knowledge, lawful decision rights and tested operational options jointly support preservation of essential services. Its claims are expressly provisional. An organization may have excellent risk documentation and still fail because the disturbance lies outside modelled conditions; it may succeed without sophisticated documentation because workers improvise effectively or external actors intervene. The framework's value lies in generating empirical questions and defensible decisions, not in assigning spurious numerical precision to an unvalidated relationship.

Figure 32.3

Conditions for accountable enterprise resilience.



Note. Author-developed conceptual synthesis. Constructs are not a statistically estimated structural model; relationships require context-specific evidence and future empirical assessment.

An ethical perspective changes what counts as resilience. Preserving commercial revenue is not a defensible success if it requires dangerous dispatch, concealed payment errors, unlawful handling of customer data or arbitrary harm to weaker suppliers. Nor should all business interruptions be treated as equally important: delivering critical medicines, wages or safe food may carry consequences different from delaying nonessential marketing activity. Ethical analysis thus informs the setting of acceptable service floors and the selection of contingencies. It does not supply an empirically measured probability, and the theoretical comparison of rights, duties and distributive justice remains the subject of Chapter 33. Chapter 34 develops an explicitly biblical perspective; this chapter retains standards of evidence and professional reasoning applicable across confessional and nonconfessional settings.

Three researchable propositions follow from the synthesis. First, the relationship between formal ERM adoption and observed recovery performance is likely to depend on whether critical cross-functional dependencies and third-party relationships are represented and tested, rather than on policy adoption alone. Second, for resource-constrained enterprises, the combination of clear decision authority, credible low-cost alternatives and repeated exercises may be more predictive of continuity than aggregate expenditure on resilience technologies. Third, under correlated systemic shocks, diversified vendors or payment channels will improve outcomes only to the extent that the supposedly independent alternatives do not share critical failure points. These are hypotheses, not reported discoveries. They invite

comparative, longitudinal and mixed-method testing capable of separating selection effects, intervention implementation and shock severity.

32.15.1 Epistemic responsibility and the politics of recovery

ERM joins questions of knowledge with questions of power. The risk analyst may provide a probability or service threshold, but governing actors decide which harms count, who is consulted, what remains undisclosed and whether residual exposure is acceptable. An apparently technical decision can therefore institutionalize a distribution of burdens. The argument for public accountability is not that every risk judgement should be made collectively; emergency decisions may require rapid delegated authority. It is that delegated authority should be traceable to legitimate purposes, proportionate constraints, meaningful challenge and a credible route to remedy. Probability cannot convert an otherwise prohibited action into a permissible one, just as a legal requirement cannot itself establish the empirical likelihood of a particular harm (OECD, 2023; Aven, 2016).

There is also an epistemological limit to the language of resilience. If an enterprise's adaptive capacity is inferred entirely from survival after an event, the measure suffers from outcome selection and obscures organizations that prepared well but met exceptionally severe conditions. Robust inquiry should differentiate ex ante preparedness, observed conduct under disturbance, realized harm, contextual shock intensity and the quality of post-event learning. It should investigate unsuccessful cases rather than rely only on celebrated survivors, and distinguish independently corroborated observations from internal narratives prepared for investors or reputation management. The conceptual diagram that follows should therefore be interpreted as a set of proposed relationships whose measures and causal identification remain open to examination, not as a universal law of organizational behaviour.

32.16 RESEARCH AGENDA AND METHODOLOGICAL DIRECTIONS

The first priority is to examine ERM *effectiveness*, not merely ERM presence. Future research could construct a panel of enterprises with repeated measurements of dependence on key suppliers, cash buffers, recovery exercises, governance quality and verified service interruptions. It would need to address survivorship bias, because firms most vulnerable to disruption may cease reporting, and selection bias, because better-governed enterprises are also more likely to adopt formal frameworks. Difference-in-differences or matched longitudinal comparisons might contribute if parallel-trend and measurement assumptions are defensible; they would not become causal simply because a sophisticated statistical procedure was used. Auditable event histories, external interruption evidence and preregistered definitions would materially improve inference (Bromiley et al., 2015; Aven, 2016).

A second agenda concerns African microenterprises, cooperatives, and informal commercial networks. Evidence from formal financial institutions cannot be assumed to explain owner-managed traders whose records, insurance access and contractual alternatives differ. Comparative case work and secondary administrative data could investigate which combinations of redundancy, flexible relationships and public infrastructure yield acceptable continuity at realistic cost. A third agenda concerns interconnected cyber, climate and payment dependencies, where network mapping and agent-based simulations may reveal threshold behaviour that independent risk registers overlook. Simulations should be calibrated against observed system constraints and clearly separated from causal empirical findings. Finally, justice-oriented resilience research should test whether interventions protect customers and workers equitably or simply transfer disruption costs to actors with less bargaining power.

Methodological replication should include a source register, operational definitions, time windows, explicit exposure denominators, machine-readable analytical formulas where possible, document versions, missing-data treatment and a clear distinction between organizational statements and independently

verified events. In crisis studies, protecting sensitive personal or security information can coexist with transparent publication of aggregate methods and deidentified evidence. The governing scholarly rule is straightforward: a model becomes credible by surviving attempts to test its assumptions and predictions, not by appearing sophisticated in a diagram.

32.17 CHAPTER SYNTHESIS AND CONCLUSION

The chapter has established risk as an objective-related consequence of uncertainty rather than an isolated list of threats; distinguished it from unknowability, vulnerability and resilience; and located enterprise risk decisions within legitimate authority and accountable information. Its functional analysis shows that strategic, financial, operating, technological, people-related, legal and systemic exposures overlap. Risk registers, matrices, expected-value models, stress tests and business impact analyses provide complementary lenses, but no single method substitutes for judgment or establishes causal effectiveness. Continuity depends on credible minimum services, realistic RTOs and RPOs, safe fallback arrangements, accessible crisis leadership, honest communication and exercised procedures. Resilience extends beyond technical restoration to financial survivability, learning, adaptation and the distributive consequences of recovery.

The worked Kigali case illustrates the difference between an event-loss estimate, a conditional resilience option and the cash needed to execute that option. Its numerical result is contingent on assumed costs and frequencies; its managerial value is the reproducible structure of the decision. The Maersk case and Rwanda's documented flood experience establish why apparently localized disturbances can travel through international logistics, information systems and public infrastructure. They do not license unsupported extrapolation from large companies to small firms or from national observations to individual enterprise histories. The most defensible conclusion is that organizational resilience is a continually tested capability to preserve legitimate commitments when expectations fail, with explicit limits on what enterprises may shift onto other people or the environment.

Table 32.9

Seven integrated conclusions for executive and scholarly use

Analytical conclusion	Practical implication
Risk is objective-related uncertainty, not a colour score	Describe consequences, assumptions and evidence quality
Enterprise exposures propagate across functions	Map shared dependencies and compound conditions
Governance makes risk-taking accountable	Specify appetite, owners, escalation and independent challenge
Financial viability and liquidity survival differ	Test cash timing as well as average expected loss
Continuity objectives are commitments, not capabilities	Demonstrate restoration times and minimum safe service through tests
Resilience combines buffers, flexibility and learning	Invest selectively, verify alternatives and adapt after incidents
Responsible recovery includes affected stakeholders	Measure safety, fairness, remedy and trust alongside service restoration

Note. Original synthesis from the chapter. Each conclusion is conditional on evidence and contextual interpretation.

32.18 KEY TERMINOLOGY

The terminology below distinguishes decision concepts from operational performance targets. Definitions are formulated for this chapter's analytical context and should be read alongside, rather than

substituted for, any formally applicable terminology in the relevant management-system standard or national legal instrument.

Table 32.10

Analytical glossary of risk, continuity, and resilience concepts

Term	Precise meaning and distinction
Business impact analysis (BIA)	Structured analysis of essential activities, dependencies and time-dependent interruption consequences used to establish recovery requirements; it does not prove that recovery is feasible.
Business continuity	Organizational capacity to maintain or resume priority activities at specified acceptable levels after disruption, supported by executable and tested arrangements.
Common-cause failure	Loss of several ostensibly independent safeguards or providers because they share an underlying vulnerability or initiating condition.
Crisis management	Strategic coordination of authority, sensemaking, communication and action during a consequential, urgent and uncertain organizational event.
Enterprise risk management (ERM)	Organization-wide arrangements for interpreting and responding to uncertainty in relation to objectives, legitimate authority and affected stakeholders.
Expected loss	Probability-weighted sum of non-overlapping and fully specified monetary outcomes under a justified probability distribution.
Inherent risk	Exposure assessed before the effect of specified treatments, with the reference scenario and assumptions explicitly stated.
Maximum tolerable period of disruption (MTPD)	Duration after which interruption consequences become unacceptable according to defined service, legal or other criteria.
Recovery point objective (RPO)	Maximum acceptable age of restored data, expressed in time; it is not the elapsed time needed to restore an application.
Recovery time objective (RTO)	Intended maximum time to restore a specified activity or resource; it is a requirement until demonstrated in a relevant test.
Residual risk	Exposure remaining after defined treatments, conditional on evidence that the controls actually operate.
Resilience	Context-dependent capacity to anticipate, cope with, recover from and adapt to disturbance while maintaining legitimate priorities and responsibilities.
Risk appetite	Types and amounts of uncertainty that authorized decision-makers are willing to accept in pursuit of objectives, within binding constraints.
Risk capacity	Degree of adverse exposure the enterprise can bear without breaching survival, solvency or other non-negotiable limits.
Scenario analysis	Examination of coherent configurations of conditions and consequences, without necessarily asserting that their probabilities are known.
Stress test	Examination of whether operations, liquidity or other essential commitments withstand severe explicitly stated conditions.
Systemic risk	Risk transmitted or amplified through shared networks, infrastructure, institutions or feedback beyond one organizational activity.

Note. These working definitions synthesize ISO (2018, 2019, 2021), Aven (2016), and Duchek (2020). Abbreviations are introduced on first use in the text and are not intended as substitutes for the issuing bodies' exact normative definitions.

32.19 ANALYTICAL QUESTIONS, APPLIED EXERCISES, AND EDUCATOR GUIDANCE

32.19.1 Foundational conceptual inquiry

A strong reading of the chapter should make students capable of explaining, rather than simply repeating, the contested boundary between measurable risk and deeper uncertainty. One foundational assessment asks the student to evaluate whether a probability estimated from short historical experience can guide a decision under structural change. Another asks for a critical comparison of a company's risk appetite with its financial risk capacity and its non-negotiable duties, using an example where expected profit cannot justify knowingly unsafe activity. Students should also explain the relationship among RPO, RTO and MTPD, showing why these measures are jointly necessary but not interchangeable. An effective response will distinguish an organizational requirement, an independently demonstrated capability and an outcome experienced by a stakeholder.

Theoretical understanding should be tested by giving students opposing claims to evaluate. One claim asserts that two suppliers must always be safer than one; the other asserts that an untested, comprehensive continuity manual offers greater protection than a short, frequently exercised procedure. The student's responsibility is to specify the assumptions under which either claim could hold, identify common-cause dependencies, and distinguish documentary compliance from demonstrated performance. At postgraduate level, students should additionally explain the tension between high-reliability and normal-accident reasoning and assess whether the chapter's conceptual framework could be falsified with longitudinal enterprise data.

32.19.2 Quantitative, diagnostic, and professional application

The Rwanda-centred case offers a reproducible application rather than a request for superficial numerical answers. Students should first rebuild the loss bridge and the event-contingent net benefit in Table 32.7, then assume that the alternative carrier protects only 40% rather than 60% of sales on days 2 to 5. Keeping other assumed terms unchanged, the avoided contribution becomes RWF 1,920,000 and the event-contingent net benefit becomes RWF 1,920,000; the resulting illustrative break-even probability is approximately 33.85%. Students should explain why holding avoided stock loss and claims constant may itself be implausible, and provide an appropriate sensitivity comparison. A second exercise reduces collections to RWF 200,000 and increases emergency supplier spending by RWF 600,000. The original five-day closing cash then becomes negative RWF 600,000, implying a RWF 2,600,000 gap relative to the RWF 2 million floor before any additional intraday financing needs. The assessment must discuss executability, not just arithmetic.

An advanced exercise should build a reverse stress test of KED's survival limit using combinations of late collections, fixed obligations, supplier costs, activation expense and service interruption. The student must specify whether costs are truly incremental, whether sources of finance are committed, and how reliance on a common payment or transport provider affects the result. An alternative diagnostic task asks learners to construct two equal ordinal heat-map scores for events with very different financial, safety and rights consequences, then explain why the multiplication of ordinal categories does not establish equal risk. The expected intellectual product is a defensible decision memo that discloses ignorance and recommends testable corrective measures.

32.19.3 Professional assessment standards and evidence of achievement

Table 32.11

Applied assessment design aligned to chapter learning outcomes

Scholarly or professional deliverable	Evidence required for an excellent submission	Main outcomes
Critical theory essay on risk and resilience	Rival explanations, explicit assumptions, boundary conditions, ethical limits and defensible synthesis	LO1, LO2, LO8
Rwandan SME continuity and board memorandum	Dependency map, five material exposures, valid BIA, at least two credible alternate arrangements, governance approvals and exercise plan	LO3, LO4, LO6, LO7
Financial loss and reverse-stress dossier	Reproducible arithmetic, daily cash timing, justified thresholds, probability sensitivity, nonmonetary constraints and transparent recommendation	LO4, LO5, LO8
Comparative evidence and research design	Critical interpretation of Mærsk and an additional documented case, valid units of analysis, confounding controls, source traceability and falsifiable propositions	LO2, LO7, LO8

Note. Assignment specifications and achievement criteria are developed for pedagogical use; they are not records of a conducted empirical study. A graduate-level submission should incorporate independent source verification, APA 7th references and a documented assumptions register.

Educators should use a progression of evidence demands rather than judge all responses by their length. At an introductory level, the assessment can focus on causal pathways, authority and critical terminology. At an intermediate level, students should demonstrate auditable calculations and reconcile losses with cash. At postgraduate level, they should test rival interpretations, confront identification problems and justify research design. Particularly strong submissions may question a convenient premise, disclose a limitation or recommend against an attractive intervention where safety, feasibility or rights are inadequately protected. The assessment rubric should reward defensible reasoning and transparent correction, rather than numerical precision unsupported by the available evidence.

32.20 FURTHER READING

For foundations of enterprise-wide risk and the critique of current practice, Bromiley et al. (2015), Aven (2016), and Mikes (2009) are especially valuable together because they address conceptual, inferential and organizational limitations. Duchek (2020) and Herbane (2010) provide complementary organizational-resilience and small-enterprise perspectives; Christopher and Peck (2004) connect resilience to network design. For professional application, ISO 31000:2018, IEC 31010:2019, ISO 22301:2019, ISO/TS 22317:2021, ISO 22361:2022, the IIA's 2026 Statements of Position and NIST CSF 2.0 should be read with attention to each instrument's legal status, intended audience and scope. Rwanda-specific contextual reading should include the NISR 2024 enterprise survey, the NBR 2024/25 annual report and current National Cyber Security Authority guidance. These materials should be updated at the time of practical use because regulatory status and technical requirements can change.

REFERENCES

A.P. Møller–Mærsk. (2017, June 28). *Cyber attack update*. https://investor.maersk.com/node/19831/pdf

A.P. Møller–Mærsk. (2018). *Annual report 2017*. https://investor.maersk.com/news-releases/news-release-details/annual-report-2017

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research, 253*(1), 1–13. https://doi.org/10.1016/j.ejor.2015.12.023

Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: The concept, a literature review and future directions. *International Journal of Production Research, 49*(18), 5375–5393. https://doi.org/10.1080/00207543.2011.563826

Boin, A., 't Hart, P., Stern, E., & Sundelius, B. (2005). *The politics of crisis management: Public leadership under pressure*. Cambridge University Press. https://doi.org/10.1017/CBO9780511490880

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. *Long Range Planning, 48*(4), 265–276. https://doi.org/10.1016/j.lrp.2014.07.005

Cantu, J., Tolk, J., Fritts, S., & Gharehyakheh, A. (2020). High reliability organization (HRO) systematic literature review: Discovery of culture as a foundational hallmark. *Journal of Contingencies and Crisis Management, 28*(4), 399–410. https://doi.org/10.1111/1468-5973.12293

Christopher, M., & Peck, H. (2004). Building the resilient supply chain. *The International Journal of Logistics Management, 15*(2), 1–14. https://doi.org/10.1108/09574090410700275

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management: Integrating with strategy and performance*. https://www.coso.org/enterprise-risk-management

Cox, L. A., Jr. (2008). What's wrong with risk matrices? *Risk Analysis, 28*(2), 497–512. https://doi.org/10.1111/j.1539-6924.2008.01030.x

Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. *Business Research, 13*(1), 215–246. https://doi.org/10.1007/s40685-019-0085-7

Government of Rwanda. (2023, May 6). *Government steps up response to flood disasters*. https://www.gov.rw/blog-detail/government-steps-up-response-to-flood-disasters

Herbane, B. (2010). Small business research: Time for a crisis-based view. *International Small Business Journal, 28*(1), 43–64. https://doi.org/10.1177/0266242609350804

Hillson, D. (2002). Extending the risk process to manage opportunities. *International Journal of Project Management, 20*(3), 235–240. https://doi.org/10.1016/S0263-7863(01)00074-6

Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics, 4*, 1–23. https://doi.org/10.1146/annurev.es.04.110173.000245

Institute of Internal Auditors. (2026a, July 8). *The role of the internal audit function in enterprise risk management* [Statement of position]. https://www.theiia.org/en/resources/statements-of-position

Institute of Internal Auditors. (2026b, July 8). *Three lines model: Assurance and advice in support of effective governance* [Statement of position]. https://www.theiia.org/en/resources/statements-of-position

International Electrotechnical Commission. (2019). *IEC 31010:2019: Risk management—Risk assessment techniques*. https://www.iso.org/standard/72140.html

International Organization for Standardization. (2017). *ISO 22316:2017: Security and resilience—Organizational resilience—Principles and attributes*. https://www.iso.org/standard/50053.html

International Organization for Standardization. (2018). *ISO 31000:2018: Risk management—Guidelines*. https://www.iso.org/standard/31000

International Organization for Standardization. (2019). *ISO 22301:2019: Security and resilience—Business continuity management systems—Requirements* (including Amendment 1:2024). https://www.iso.org/standard/75106.html

International Organization for Standardization. (2021). *ISO/TS 22317:2021: Security and resilience—Business continuity management systems—Guidelines for business impact analysis*. https://www.iso.org/standard/79000.html

International Organization for Standardization. (2022). *ISO 22361:2022: Security and resilience—Crisis management—Guidelines*. https://www.iso.org/standard/50267.html

Jüttner, U., Peck, H., & Christopher, M. (2003). Supply chain risk management: Outlining an agenda for future research. *International Journal of Logistics Research and Applications, 6*(4), 197–210. https://doi.org/10.1080/1367556031000162701 6

Kaplan, R. S., & Mikes, A. (2012). Managing risks: A new framework. *Harvard Business Review, 90*(6), 48–60. https://hbr.org/2012/06/managing-risks-a-new-framework

Knight, F. H. (1921). *Risk, uncertainty and profit*. Houghton Mifflin. https://www.econlib.org/library/Knight/knRUP.html

Lengnick-Hall, C. A., Beck, T. E., & Lengnick-Hall, M. L. (2011). Developing a capacity for organizational resilience through strategic human resource management. *Human Resource Management Review, 21*(3), 243–255. https://doi.org/10.1016/j.hrmr.2010.07.001

March, J. G., & Shapira, Z. (1987). Managerial perspectives on risk and risk taking. *Management Science, 33*(11), 1404–1418. https://doi.org/10.1287/mnsc.33.11.1404

Mikes, A. (2009). Risk management and calculative cultures. *Management Accounting Research, 20*(1), 18–40. https://doi.org/10.1016/j.mar.2008.10.005

National Bank of Rwanda. (2025). *Annual report 2024/25*. https://www.bnr.rw/anreports

National Cyber Security Authority. (2024). *National cybersecurity strategy of the Republic of Rwanda 2024–2029*. https://cyber.gov.rw/rw/guidance/documentation

National Institute of Statistics of Rwanda. (2026). *Integrated business enterprise survey (2024)* [Publication tables and report updated March 6, 2026]. https://www.statistics.gov.rw/statistical-publications/business-establishment-finance-trade/business-establishment-finance-trade/integrated-business-enterprise-survey-2024

Organisation for Economic Co-operation and Development. (2023). *G20/OECD principles of corporate governance 2023*. OECD Publishing. https://doi.org/10.1787/ed750b30-en

Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST cybersecurity framework (CSF) 2.0* (NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Pearson, C. M., & Clair, J. A. (1998). Reframing crisis management. *Academy of Management Review, 23*(1), 59–76. https://doi.org/10.5465/amr.1998.192960

Perrow, C. (1984). *Normal accidents: Living with high-risk technologies*. Basic Books. https://search.worldcat.org/title/10229932

Ponomarov, S. Y., & Holcomb, M. C. (2009). Understanding the concept of supply chain resilience. *The International Journal of Logistics Management, 20*(1), 124–143. https://doi.org/10.1108/09574090910954873

Repenning, N. P., & Sterman, J. D. (2001). Nobody ever gets credit for fixing problems that never happened: Creating and sustaining process improvement. *California Management Review, 43*(4), 64–88. https://doi.org/10.2307/41166101

Republic of Rwanda. (2021). *Law No. 058/2021 of 13/10/2021 relating to the protection of personal data and privacy* (Official Gazette, Special Issue of October 15, 2021). https://dpo.gov.rw/fileadmin/DPO/Law_relating_to_the_protection_of_personal_data_and_privacy.pdf

Sheffi, Y., & Rice, J. B., Jr. (2005). A supply chain view of the resilient enterprise. *MIT Sloan Management Review, 47*(1), 41–48. https://shop.sloanreview.mit.edu/store/a-supply-chain-view-of-the-resilient-enterprise

United Nations Office for Disaster Risk Reduction. (2015). *Sendai framework for disaster risk reduction 2015–2030*. https://www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030

Weick, K. E. (1988). Enacted sensemaking in crisis situations. *Journal of Management Studies, 25*(4), 305–317. https://doi.org/10.1111/j.1467-6486.1988.tb00039.x

Weick, K. E., & Sutcliffe, K. M. (2015). *Managing the unexpected: Sustained performance in a complex world* (3rd ed.). Jossey-Bass. https://doi.org/10.1002/9781119175834

Wieland, A., & Wallenburg, C. M. (2013). The influence of relational competencies on supply chain resilience: A relational view. *International Journal of Physical Distribution & Logistics Management, 43*(4), 300–320. https://doi.org/10.1108/IJPDLM-08-2012-0243